NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MAINTAINING INTEROPERABILITY IN A TARGET-RICH ENVIRONMENT

by

Mei Ling Venessa Ng

September 2012

Thesis Advisors:	Gary O. Langford Oleg A. Yakimenko
Second Reader:	John S. Osmundson

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Maintaining Interoperability in a Target-Rich Environment		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Mei Ling Venessa Ng			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			

13. ABSTRACT

Achieving interoperability in a net-centric environment is fundamental to maximizing the potential of information sharing and effective use of resources in military operations. With the increasing reliance on unmanned platforms worldwide, there is a need to study the limitations of existing Command and Control (C2) Systems in dealing with the increasing number of objects. More processing power would be required to achieve or maintain a certain level of efficiency and effectiveness of the C2 system in managing and processing the tracks detected. Also, with increasing collaborations between services and allies, interoperability between multiple systems is pertinent. An additional challenge is the need to exchange target-rich tactical picture information.

A systems engineering approach was used to identify the critical factors necessary in a C2 system to be architected to satisfy the needs for a future C2 system able to achieve and maintain interoperability in a target rich environment. A pilot study was conducted using ExtendSim to model growing networks and injection of increased amounts of data to assess their impact on the timeliness of information received by the system nodes. Potential future work on the pilot study was described.

14. SUBJECT TERMS Interoperability, Command and Control (C2), net-centric, network-centric warfare			**15. NUMBER OF PAGES** 140
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MAINTAINING INTEROPERABILITY IN A TARGET-RICH ENVIRONMENT

Mei Ling Venessa Ng
Civilian, Defence Science & Technology Agency, Singapore
B.Eng (Electrical Engineering), National University of Singapore, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Mei Ling Venessa Ng

Approved by: Gary O. Langford
Thesis Advisor

Oleg A. Yakimenko
Co-Advisor

John S. Osmundson
Second Reader

Clifford A. Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Achieving interoperability in a net-centric environment is fundamental to maximizing the potential of information sharing and effective use of resources in military operations. With the increasing reliance on unmanned platforms worldwide, there is a need to study the limitations of existing Command and Control (C2) Systems in dealing with the increasing number of objects. More processing power would be required to achieve or maintain a certain level of efficiency and effectiveness of the C2 system in managing and processing the tracks detected. Also, with increasing collaborations between services and allies, interoperability between multiple systems is pertinent. An additional challenge is the need to exchange target-rich tactical picture information.

A systems engineering approach was used to identify the critical factors necessary in a C2 system to be architected to satisfy the needs for a future C2 system able to achieve and maintain interoperability in a target rich environment. A pilot study was conducted using ExtendSim to model growing networks and injection of increased amounts of data to assess their impact on the timeliness of information received by the system nodes. Potential future work on the pilot study was described.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. WHAT IS INTEROPERABILITY? 1
1. Ontology 6
2. Stability 7
3. Command and Control 9
4. Integration 10
5. Trust 12

II. BACKGROUND 13
A. GENERAL NATURE OF COMMAND AND CONTROL 13
1. C2 Definitions 13
2. C2 Functional Decomposition 14
3. Goals of a C2 System 15
B. EVOLUTION OF COMMAND AND OF CONTROL 16
C. DISCUSSION OF PROBLEM DUE TO INCREASING RELIANCE ON UNMANNED SYSTEMS 17
D. PROBLEMS ASSOCIATED WITH LIMITATIONS OF EXISTING SYSTEMS TO DEAL WITH INCREASING NUMBER OF OBJECTS 18
1. Increasing Complexity and Interconnectedness 18
2. Technological Limitations 19
E. GOVERNANCE CHALLENGES 20

III. PROBLEM DEFINITION 23
A. PROBLEM DECOMPOSITION 23
1. System of Systems 23
2. Network-Centric Warfare 24
3. Target-Rich Environment 26
B. BOUNDARIES & BOUNDARY CONDITIONS 27
1. Physical Boundaries 27
a. Geographical Location of the SoS Deployment 27
b. Operating Range of Systems 28
2. Functional Boundaries 28
a. To Communicate 28
b. To Command 29
c. To Control 29
d. To Propagate Information 30
e. To Process Information 30
3. Behavioral Boundaries 30
a. SoS Emergence 30
b. Governance of Systems 31
c. Data/Information Propagation 32
C. LIMITATIONS AND CONSTRAINTS 32

1. Limitations 33
a. Operational Space 33
b. Control 33
c. Component System Performance 33
2. Constraints 34
a. Command and Control (C2) 34
b. Policies 34
D. SCOPE 34
E. PROCESS DECOMPOSITION 35

IV. DEVELOPMENT OF SOLUTION 37
A. NETWORK CONTROL THEORY 37
B. APPROACH AND METHOD 40
C. PRINCIPLES 40
D. HEURISTICS 41

V. A FUTURE COMMAND AND CONTROL SYSTEM 43
A. FUTURE COMMAND AND CONTROL 43
1. A Science of Command and Control 43
B. NEED FOR INTEROPERABILITY 43
1. Levels of Interoperability 44
2. NCW Maturity Model 45
C. KEY FACTORS REQUIRED FOR INTEROPERABILITY 46
1. Network Architecture 47
a. System Interactions 47
b. Use of Common/Open Architecture 49
2. Command and Control (C2) 51
a. C2 Systems 51
b. C2 Hierarchy 52
3. Use of Common Ontology within System of Systems 53
4. Systems Integration 54
a. System-to-System Connection/Coupling/Cohesion 54
b. Legacy vs. New Systems 55
c. Integration Testing 55
5. System Stability 56
a. Local and Global Stability 56
b. Operator Training 57
6. Information Security 57
7. Concept of Operations 59
8. Management of Change Requirements 60

VI. MODELING OF MULTI-SYSTEM AND TARGET-RICH ENVIRONMENT ... 61
A. PROBLEM 61
B. BACKGROUND 61
C. APPROACH AND ASSUMPTIONS 61
D. SOFTWARE USED 63
E. HARDWARE USED 64

F. MODEL DESCRIPTION 64
1. Single-Channel Data Transmission Network Model 64
2. Dual-Channel Data Transmission Network Model 74
VII. DISCUSSION OF RESULTS 77
A. PERFORMANCE METRICS 77
B. CONDUCT OF EXPERIMENTS 78
C. USE OF SINGLE CHANNEL FOR DATA TRANSMISSION 79
D. USE OF DUAL CHANNELS FOR DATA TRANSMISSION 86
E. DISCUSSION OF FUTURE WORK 91
1. Possible Improvements to SoS Network Architecture Model 91
2. Comparison with Other Network Architecture Models 92
3. Quality Loss Function Analysis 93
VIII. CONCLUSION 95
APPENDIX I: SUGGESTED ELEMENTS OF AN ADVANCED NAVAL INFORMATION ASSURANCE RESEARCH PROGRAM 99
APPENDIX II 101
A. EXTENDSIM MODELS FOR VARYING LAYERS OF SYSTEM NODES IN SINGLE-CHANNEL FOR DATA EXCHANGE 101
B. EXTENDSIM MODELS FOR VARYING LAYERS OF SYSTEM NODES IN DUAL-CHANNELS FOR DATA EXCHANGE 106
LIST OF REFERENCES 111
GENERAL READING REFERENCES 115
INITIAL DISTRIBUTION LIST 117

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Illustration of System of Systems Interoperability (After Langford, 2012) 3
Figure 2. Example of System of Systems – Naval Integrated Fire Control (From Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, 2008) 5
Figure 3. "Use Knowledge" Functional Decomposition 14
Figure 4. Architectures for Centralized, Decentralized and Distributed Control Architectures (From Jin, 2007) 37
Figure 5. Diagram of a Typical Networked Control System (From Jin, 2007) ... 38
Figure 6. Block Diagram Model of An Autonomous Switching Hybrid System (From Ding, 2009) 39
Figure 7. Network-Centric Warfare Tenets (From Alberts & Hayes, 2003) 44
Figure 8. NCW Maturity Model (From Alberts & Hayes, 2003) 45
Figure 9. Hybrid Star-Bus Network Topology (From Hsieh, 2012) 48
Figure 10. Generic System Node H-Block and Sub-Components 67
Figure 11. Generic System Node Processor Segment 67
Figure 12. Generic System Node Message Forwarding/Feedback Segment 68
Figure 13. Message Generating H-Block and Sub-Components 69
Figure 14. Message Generator / Processor Segment of Message Generating System Node 69
Figure 15. Message Forwarding / Feedback Collection Segment of Message Generating System Node 70
Figure 16. SoS Network Architecture of 7 System Nodes 71
Figure 17. SoS Network Architecture of 75 System Nodes 72
Figure 18. Modified SoS Network Architecture of 7-Node System 76
Figure 19. Distribution of Message Propagation Time in Single Channel SoS Network Model 80
Figure 20. Trend Breakdown of Mean Time for Data-Packages to Reach End-Nodes for Varying Number of Layers of System Nodes 81
Figure 21. Trend Breakdown of Mean Time for Data-Packages to Reach End-Nodes for Varying Number of Messages 82
Figure 22. Trend of Message Propagation Time vs. Number of Node Layers and Messages in SoS 83
Figure 23. Distribution of Message Propagation Time for Data-Package to Return to Origin in Single Channel SoS Network Model 84
Figure 24. Trend Breakdown of Mean Time for Data-Packages to Arrive Back at Origin for Varying Number of Layers of Nodes 85
Figure 25. Trend Breakdown of Mean Time for Data-Packages to Arrive Back at Origin for Varying Number of Messages 86
Figure 26. Distribution of Message Propagation Time in Single Channel SoS Network Model (Satellite Model) 88

Figure 27. Trend Breakdown of Mean Time for Data-Packages to Reach End-Nodes for Varying Number of Layers of System Nodes (Satellite Model) 88
Figure 28. Trend Breakdown of Mean Time for Data-Packages to Arrive Back at Origin for Varying Number of Messages (Satellite Model) 89
Figure 29. ExtendSim Network Model of 3 Generic System Nodes (2 Layers) . 101
Figure 30. ExtendSim Network Model of 7 Generic System Nodes (3 Layers) . 102
Figure 31. ExtendSim Network Model of 15 Generic System Nodes (4 Layers) 103
Figure 32. ExtendSim Network Model of 31 Generic System Nodes (5 Layers) 104
Figure 33. ExtendSim Network Model of 63 Generic System Nodes (6 Layers) 105
Figure 34. Modified ExtendSim Network Model of 3 Generic System Nodes (2 Layers) 106
Figure 35. Modified ExtendSim Network Model of 7 Generic System Nodes (3 Layers) 107
Figure 36. Modified ExtendSim Network Model of 15 Generic System Nodes (4 Layers) 108
Figure 37. Modified ExtendSim Network Model of 31 Generic System Nodes (5 Layers) 109
Figure 38. Modified ExtendSim Network Model of 63 Generic System Nodes (6 Layers) 110

LIST OF TABLES

Table 1. System Node H-Block Connection Representations 65
Table 2. Number of System Nodes Corresponding to Number of Layers in SoS Network 73
Table 3. Performance Metrics Description 77
Table 4. Average Elapsed Time to Arrive at End-Nodes 79
Table 5. Maximum Elapsed Time to Arrive at End-Nodes 82
Table 6. Average Elapsed Time to Propagate to End-Nodes and Return to Message Generating Node 84
Table 7. Average Elapsed Time to Arrive at End-Nodes for Satellite Model 87
Table 8. Average Elapsed Time to Propagate to End-Nodes and Return to Message Generating Node for Satellite Model 89
Table 9. Information Assurance Elements (From Committee on Information Assurance for Network-Centric Naval Forces, 2010, p. 89)..... 100

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

EA	Enterprise Architecture
C2	Command and Control
CNO	Chief of Naval Operations
CONOPS	Concept of Operations
COTS	Commercial-Off-the-Shelf
DoD	U.S. Department of Defense
EMMI	Energy, Matter, Material Wealth and Information
GLS	General Living Systems
GST	General Systems Theory
H-Block	Hierarchical Block
IA	Information Assurance
ISR	Intelligence, Surveillance and Reconnaissance
LAN	Local Area Network
LOS	Line-of-Sight
NATO	North Atlantic Treaty Organization
NCS	Networked Control System
NCW	Net-Centric or Network-Centric Warfare
OA	Open Architecture
OEM	Original Equipment Manufacturer
OPNAV	Office of Naval Operations Staff
OV	Operational View
RAM	Read-Access Memory
SoS	System of Systems
TPED	Tasking, Production, Exploitation and Dissemination
UMS	Unmanned System
VMF	Variable Message Format
WAN	Wide Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Achieving interoperability in a net-centric environment is fundamental to maximizing the potential of information sharing and effective use of resources in military operations. With the increasing reliance on unmanned platforms and use of highly complex and interconnected systems worldwide, there is a need to study the limitations of existing Command and Control (C2) systems in dealing with the increasing number of objects in the military domain.

An analogy was drawn between systems interoperability and the inter-relationships between humans at work to identify the factors that could affect the effectiveness and efficiency of system-to-system interoperability. These factors included network architecture, command and control, common ontology, systems integration, systems stability, information security, concept of operations, and management of change requirements. Using a systems engineering approach, the problem of establishing and maintaining multi-system interoperability in a target-rich environment was decomposed, further evaluated using the identified elements of interoperability, and addressed by allocating suitable processes to the problem components through the use of process decomposition.

An ExtendSim model was designed and developed to simulate a multi-system and multi-target environment transmission network model to study the issue of increasing number of systems in the system of systems (SoS) network and an increasingly congested environment. The model used the discrete modeling capability of the software to achieve a network able to propagate items from a starting system node to the other system nodes, with the items representing the data/information packages sent. The network model was evaluated using single and dual channel transmission, in which the data/information sending and feedback replies were sent on the same network path for the first simulation run and via separate paths for the next simulation run respectively. It was found that for the dual channel transmission configuration, the time delay incurred for the propagation of messages to all the nodes in the

system followed a near-linear incremental trend, which is an improvement from the exponential time delay incurred for the single channel transmission network model. With this, the time incurred for an overall communications loop between two systems, with multiple systems linked between them, was observed to be shorter for a dual channel transmission than a single channel transmission. Thus, to handle the increasing number of participating systems in the SoS and increasing number of targets in the environment, a secondary channel supporting the direct feedback of messages, such as a satellite link, would reduce the overall time delayed for messages to reach all systems and return to the originating system node.

Future work includes parameter modifications to the existing network models to make them more realistic and applicable to other types of information transmission, comparison of the network models against other types of network models and performing quality loss function analysis on existing results to examine how much stakeholders are willing to pay for modifications to C2 network architectures to improve its performance and thus, support critical decision making.

ACKNOWLEDGMENTS

This thesis would not have been possible without the steady guidance, patience and reassurance of my thesis advisor, Mr Gary Langford. Working on this project has helped me view C2 from multiple aspects and your advice has been invaluable in triggering my thought process and helped me focus on the key ideas to integration that had been useful in this thesis.

I would also like to thank my co-advisor, Mr Oleg Yakimenko, for his insights, encouragement and guidance. Thanks also to my second reader, Dr. John Osmundson, for all the support he has rendered me.

I would also like to extend my gratitude to Mr Juan Gonzalez for his technical support, without which the modeling and simulation would not have been possible.

Finally, I wish to express my thanks to my husband and family, who are in Singapore, for their love, continued support and encouragement during the course of my studies in the Naval Postgraduate School. And also, to the new friends whom I have met during my course of studies, thank you for the company and friendship, it has been an unforgettable time.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Achieving interoperability in a network-centric environment is fundamental to maximizing the effectiveness in information sharing between entities and use of resources in military operations. This is especially true for the warfare of today in which network-centric warfare is seen as a force-multiplier (Alberts, Garstka, & Stein, Network centric warfare: developing and leveraging information superiority, 1999) (Department of Defense, 2009) through effectively linking knowledgeable entities in the battlespace. In the U.S. Department of Defense (DoD), network-centricity or "net-centricity is defined as the ability to provide a framework for full human and technical interoperability that (1) allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence and (2) protects information from those who should not have it." Network-centric warfare is described by Alberts et al., as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization (1999).

> As more and more systems are integrated into DoD's net centric environment, information technology systems are evolving from sets of individual systems to sets of services that work in different combinations to meet different user needs. Work is needed to specifically address the issues of systems engineering in net-centric enterprise systems. (Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, 2008).

A. WHAT IS INTEROPERABILITY?

Interoperability is the ability of systems, units or forces to provide data and information to and accept the same from other systems, units or forces and to use the data and information so exchanged to enable these entities to operate together to achieve a common goal. These systems are integrated to form

outcomes such that they are able to achieve much more together than what individual systems can do on their own or by multiple systems acting individually. (Langford, 2012) segregates between integration and interaction as follows:

- Integration provides adoption of ideas and causal changes
- Interaction offers only the potential for integration

> The whole is crucially greater than the sum of its parts. Integration makes things happen faster with individual interacting objects. (Langford, 2012)

> IT and NSS (National Security Systems) interoperability includes both the technical exchange of information and the operational effectiveness of that exchanged information as required for mission accomplishment. Interoperability includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with Information Assurance. (Joint Chiefs of Staff, 2012)

Interoperability between systems or force units within a battlespace allows for information and intelligence sharing which would help enhance overall situational awareness of these units and give them the information superiority edge so as to achieve better mission success.

Interoperability between systems can be depicted as shown in Figure 1. Triangles illustrate the existing system (corresponding to the triangle below) and “wanted” system (corresponding to the triangle above). The purpose of the integration between these systems is to achieve the new capability only achievable from the integration (as depicted by the overlapping region between the 2 system triangles). The capability is driven by the mission requirements and constrained by the standards applicable to these types of systems. The requirements of the missions would also influence the interoperability required between these systems, subject to the capabilities of the new and existing system. Through correct, timely and meaningful exchange of energy, matter,

material wealth and information (EMMI[1]) between the "want" and "have" systems, these systems can then be able to connect, send and receive data/information between systems. The information exchange and use of the information to execute individual system actions towards achieving the ultimate goal of the mission would signify there is cohesion and coupling between the systems. With this interaction (connection, cohesion and coupling) between the systems, interoperability between these systems can then occur.

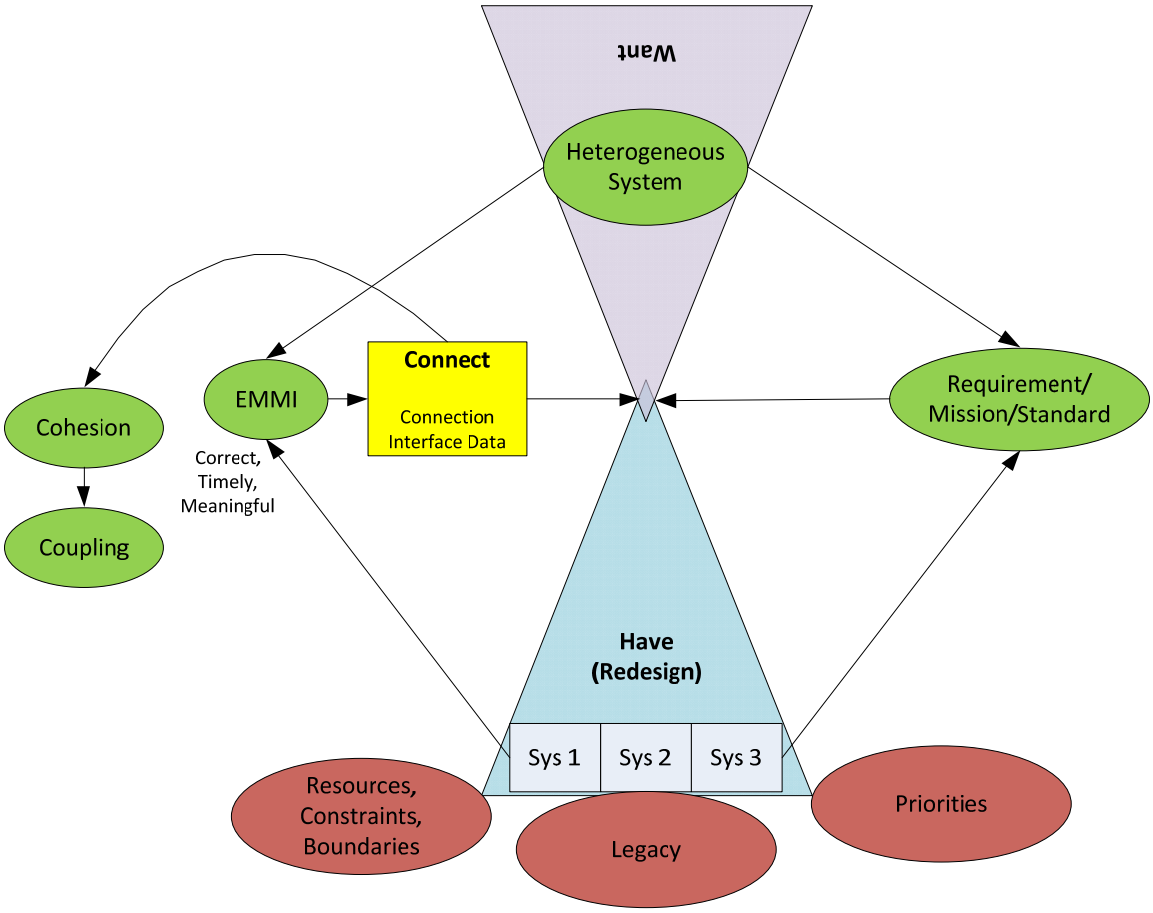

Figure 1. Illustration of System of Systems Interoperability (After Langford, 2012)

Interoperability can also be viewed in the context of individuals working together in a company—the ability of individual people working together to

[1] Energy, Matter, Material Wealth and Information (EMMI) is a term coined by Langford (2012) to express the interactions between objects.

achieve a company's goal of progress through data or information sharing and exchange. Maintaining discipline and order in an organization is captured in the function of 'to manage', i.e., command, control, communication, organization, planning, and team-building. All of these functions help with discipline and order. Additionally, the individual behaviors are also important. Behaviors derive from the organization's environment and constraints as well as outside influences. These outside influences are referred to as externalities. Both systemic characteristics and externalities influence command and control from a perspective of discipline and order (Liebowitz & Margolis, 2012).

The intricacies and dynamism in human working relationships are analogous to that of an environment in which systems work together to function better both individually and as a system of systems. For example, in their jobs, individuals are required to fulfill tasks related to their job scopes and these individuals (or systems) work on projects singly or in groups (systems of systems). These projects form a larger system of system, all in to help support the organization both in its operations.

Interoperability occurs between systems in a system of systems (SoS) configuration, where heterogeneous systems are able to operate both individually and as a group of systems, coming together to achieve a common mission or purpose. Heterogeneous is defined as composed of unrelated or differing parts or elements (*Heterogeneous, n.d.*). Gideon, Dagli and Miller (2005) described that a system of systems comprise of component systems that produce some utility together that is greater than the sum of the individual component systems. Thus, with different systems of different functionalities and capabilities collaborating, this heterogeneous combination could possibly provide the dynamic capability of the systems in the network to accomplish tasks that a group of similar systems would not be able to accomplish on their own.

Figure 2. gives an operational view[2] (OV-1) of a Naval Integrated Fire Control System in which several systems (geographically dispersed) are integrated via communication links for information and data exchange to perform the counter air mission as a united system. NATO's Integrated Air and Missile Defense System comprises of sensors, command and control facilities and weapons systems, such as surface-based air defense and fighter aircraft, similar to the illustration shown in Figure 2. This Integrated Air and Missile Defense System came to be after NATO nations participating in the military structure realized in the 1970s that national air defense systems operating independently were not as effective or efficient in protecting against air attack as they might be if operating in a more collective manner (North Atlantic Treaty Organization, 2012).

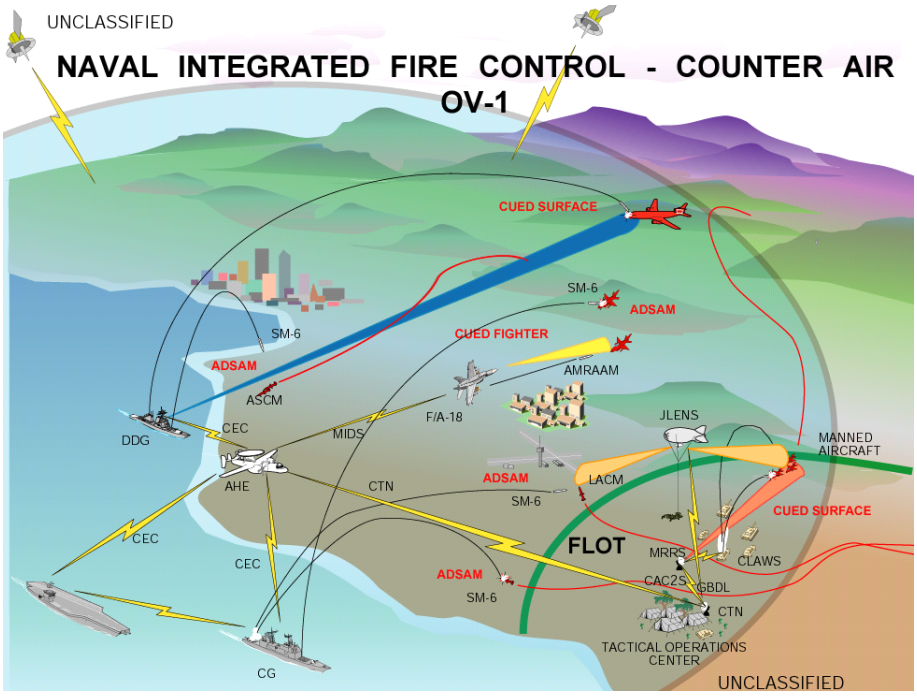

Figure 2. Example of System of Systems – Naval Integrated Fire Control (From Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, 2008)

[2] An operational view (OV) is one of views defined in the Department of Defense Architecture Framework V1.5 (DoDAF) and identifies what needs to be accomplished and who does it. OV-1 provides the high-level operational concept graphic to describe what an architecture is supposed to do, and how it is supposed to do it (Department of Defense, 2007).

> Interoperability does not emerge immediately and obviously as a core warfighting need as does fightpower, mobility, or command and control. This could result in a lack of guiding oversight and of appropriate incentives resulting in sub-optimal choices based upon local motivations. (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2009)

Thus, for interoperability to be feasible, an authority (as a form of control) oversees the planning of an interoperability roadmap and development or acquisition of military systems, so that existing and new systems could assimilate into the integration of the systems for interoperability, whilst still being able to meet future mission needs.

In addition, with increasing reliance on unmanned systems in the battlefields (as will be covered in Section II), there is a greater need to ensure more effective and efficient collaboration between these systems, manned or unmanned. As discussed, interoperability between humans in a work environment is analogous to the interaction between systems in a SoS configuration. Elements, which could impact the interrelationships between systems as they affect humans, include ontology, communications network, command and control between these systems, operational stability of individual systems and the integration between them. The following section illustrates how these elements are important in contributing to the interoperability of systems when they operate in a SoS setup.

1. Ontology

Ontology is a description (like a formal specification of a program) of the concepts and relationships that can exist for an entity or a community of entities (Gruber, n.d.) and is a conceptual model that embodies information to enable information sharing and reuse. The description of ontology includes defined items, properties of those items, concepts that relate those items, rules that govern the inclusion or exclusion of those items, terminology that is restrictive (with regards to those items) and the relationships between those items.

Ontology provides for classifications of items under multiple categories as well as identification and selection based on definitions, properties, concepts, rules, terminology and relations.

In dealing with interoperability, C2 ontology helps create a semantic representation of data and the links between these data, which will provide a framework to facilitate and regulate the information exchange between systems in C2 architecture. Accessing heterogeneous and distributed informational resources in a coordinated and virtual way requires appropriate semantic interoperability techniques to enable seamless access and retrieval of the right information resources, while preserving the information representation and management requirements for entities involved in the C2 architecture.

2. Stability

In control theory, system stability is extremely important and is generally a safety issue in the engineering of a system. The stability of a system relates to its responses to inputs or disturbances (Beardmore, 2006).

Stability can also be thought of as a change in a "state" which has certain properties that are desirable to maintain. Langford (2012) describes,

> For a system to exist and sustain itself as a system, it requires some semblance of metastability of stability to continue as a system… Metastability is the intrinsic property of a group of objects that persists in an apparent equilibrium of interactions between objects where only a small disturbance in the established interaction can dramatically change (reduce or increase) the system's lifetime.

Stability is desired in operational systems, especially military systems that have safety implications such as fire control systems, which when unstable (e.g., "opening-firing" when not commanded to), could result in potentially catastrophic consequences. Stability is required both locally in individual systems and globally in the SoS configuration. Local system stability is important to ensure that when an individual system joins a network of systems, it would continue to operate in a stable mode, albeit working together with other systems and more importantly, its

entry into the systems network would not disrupt operations. Conversely, when individual systems exit from the SoS network, these systems should continue to maintain stable operations and the remaining group of systems should continue to operate stably. Stability is also required in the medium by which these systems are connected, namely the network. If the network does not operate in a stable state, packets of information could be lost throughout the network, resulting in corrupted or incomplete data when received by the receiving system node. These are not desirable.

Rechtin (1991) proposed that “complex systems will develop and evolve within an overall architecture much more rapidly if there are stable intermediate forms than if there are not,” in the context of a large architectural framework with top-down partitioning into stable elements. Having stable intermediate forms can help ensure some stability in the complex system by only proceeding on to the next step of systems integration. (from the simplest configuration to the more complex) when the previous step works. (Maier M. W., 1999) elaborated that the stability of intermediate forms means that the intermediate forms (or individual systems) should already be capable of operating and fulfilling useful purposes prior to full deployment or construction in a larger configuration of system of systems. This idea of system evolution would provide some check on the overall stability of the integrated SoS as it grows larger.

> For a system to exist and sustain itself as a system, it requires a semblance of metastability or stability to continue as a system… Metastability is the intrinsic property of a group of objects that persists in an apparent equilibrium of interactions between objects where only a small disturbance in the established interaction can dramatically change (reduce or increase) the system’s lifetime. (Maier, 1999)

Systems are mostly metastable within the lifespan of the system. However, the larger and more complex systems become, they become increasingly sensitive to the slight disturbances, like galactic nebulae. Thus, care

should be taken in the integration planning, design and implementation to ensure that as the system of systems evolves, the overall system will remain at least metastable over its lifetime.

3. Command and Control

Command and control is defined by the Research and Technology Organisation, North Atlantic Treaty Organisation (2004) as: “The organization, process, procedures and systems necessary to allow timely political and military commander to direct and control military forces.” C2 systems are defined to include: headquarters’ facilities, information systems, sensors and warning installations and communications.

Command and control are subfunctions of the function “to manage” and can be decomposed as follows:

To command:

- To performing the art of assigning missions
- To provide resources (analyze and prioritize)
- To direct subordinates (guide, set policy and focus the force to accomplish clear objectives)
- To analyze risk (identify and assess)

To control:

- To define limits
- To negotiate
- To deal with constraints
- To determine requirements
- To allocate resources
- To report
- To maintain performance (monitor, identify and correct deviations from guidance)

Command and control are thus key elements to ensuring that there is regularity in the processes and procedures needed to be undertaken when

several systems are interoperating directly or indirectly to achieve a common goal. With the increasing reliance on unmanned systems to undertake jobs that are better suited for them to undertake, the more stringent "command" and "control" have to be to ensure that these systems are able to complement the manned systems in accomplishing the ultimate missions.

4. Integration[3]

Systems integration is the unification of the objects and their interactions of energy, matter, material wealth and information (EMMI) to provide system-level functionalities and performances. Integration between systems occurs when there is a need to fulfill a new operational need that existing or standalone systems are unable to meet. To facilitate the integration, existing systems would have to be redesigned or updated so that they would be able to connect to and communicate with other systems (which could be new).

> Integrating a system into a system of systems results in a set of systems that are both integrated and interoperable to achieve a set of metasystem functions in which all the component systems participate (to a varying degree). (Langford, 2012)

However, when two systems are integrated, both systems inevitably give up some form of flexibility in their operation and autonomous behavior.

Integration of heterogeneous information systems, databases, application software, enterprise processes and network protocols are important to facilitate sharing of what is needed by others in a system or SoS. For this to happen, there must be consistency in their nomenclature, symbology, interaction conventions, or any of a host of other human interface variations among individual systems. However, enforcing semantic consistency could create challenges in the usability of the SoS as well as in the training pipeline needed to instill required skill sets (Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, 2008). The aim of semantic

[3] In this thesis, the term "systems integration" is used interchangeably with "integration."

interoperability is the explicit ability to associate and compare different concepts on the basis of their semantic structures and relations. Once the ability to associate and the ability to compare concepts is established and sustained in a stable environment, semantic interoperability is achievable. Integrative structures and process provide those abilities.

Semantic integration is treated as a category of concepts of individual and organizational activities (such as communications, workflow and decision-making). Thinking of process as a developmental sequence of acts or activities, a theory of process consists of an explanation of how and why a process unfolds over time. At issue is the reciprocity of interoperability. Accordingly, if entity A sends data to entity B (with information exchange to carry out expected intent), then entity B must do the same for entity A. However, a change in B due to A's sending or B's receiving at the resource level may negate the ability for either entity to exchange information or to carry out their intentions. In this case, the degree of change in a process that results in a change in a system's resource ontology may not allow for backward interoperability. The definition of interoperability must hold for backward interoperability (the simple, first order test of a good definition for interoperability). Emergence still occurs without reciprocity between entities A and B. This can be determined through identifying if that object has had a loss, i.e., an interaction has occurred and thus there was emergence. Integration has also occurred when there is any form of reciprocity. If only one object has a loss (i.e., there is no reciprocity), then there is not interoperability between the two entities. Thus, the definition of interoperability needs to incorporate the concept of reciprocity, which is easily handled at the enterprise level ontology. Dealing with the system-level or system of systems-wide level of interoperability requires integration of semantics and ontology through integration.

5. Trust

Trust is an important component to enable C2 systems' interoperability with each other. Systems have to establish trust with other systems in the network of systems, such as C2 systems, before being able to join the network and commence information exchange. Trust is required for the enabling of systems to communicate and interoperate. Depending on the type of mission and information being exchanged amongst systems, the system of systems are likely to be protected from the rest of the world—the exchanged information or data should be kept within the network such that others outside the system network who are not authorized are not able to access the information. This includes both enemies and own-force systems that do not require such information, perhaps due to hierarchical restrictions.

Although, for systems to communicate or operate within the net of systems, they would require the same communication medium and ontological similarity in their system interfaces, to prevent illegal interception of information exchange and hacking of systems, security measures such as encryption and firewalls would have to be incorporated into the system integration design. This is especially important with the increasing number of systems being included in the system of systems, as it would be difficult to track and identify every system within the entire network.

This thesis assessed how a greater level of interoperability can be achieved by analyzing the specific issues that will thwart data exchange, limit or constrain throughput and degrade the effects of integration.

II. BACKGROUND

A. GENERAL NATURE OF COMMAND AND CONTROL

1. C2 Definitions

The terms “command,” “control” and “command and control” have been and are still being used exhaustively in military doctrines and operational vocabulary. However, there are varying ways and circumstances in which these words are being used, due to the lack of adequately defining these terms (Pigeau & McCann, 2002), which is evident in how the military (i.e., Navy, Air Force, Army, joint and coalition forces) has been conducting their missions and the C2 literature written so far.

Some branches of the military adopt the idea of mission command while others endorse a philosophy of centralized control and decentralized execution. Some view command and control as the same for practical purposes—in that “control is inherent in command” (Joint Chiefs of Staff, 2001).

NATO, on the other hand, defines command and control as: “the organisation, process, procedures and systems necessary to allow timely political and military decision-making and to enable military commanders to direct and control military forces.” C2 systems are defined to include headquarters’ facilities, information systems, sensors and warning installations, and communications (Research and Technology Organisation, North Atlantic Treaty Organisation, 2004).

The Department of Defense Dictionary of Military and Associated Terms (Joint Chiefs of Staff, 2010) defines command and control to be “the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.”

Pigeau and McCann (2002) describe command and control as:

> The essence of control lies in structure and process, while the essence of command lies in creativity and will… Command and control are (also considered) to be complementary – command cannot be exercised without control, but control is meaningless without command. Command creates and changes the structures and processes of control to suit the uncertain military situation, thus making command pre-eminent. Control should always be subordinate to command.

With disparate definitions of "command," "control," and "command and control," and the shift of military operations towards network-centric warfare (NCW), it would only be beneficial to have common and consistent definitions of these terms.

2. C2 Functional Decomposition

The key ingredient in a C2 system is knowledge. Knowledge is an integration of information and data. Thus, C2 is integration of its processes. Being able to acquire, manage, advance, apply and integrate knowledge within a C2 system or system of systems would allow for better situational awareness. This would thereby result in better decision fitnes[4] and decisions. The knowledge that is required for the best C2 system can be described in the following functional decomposition:

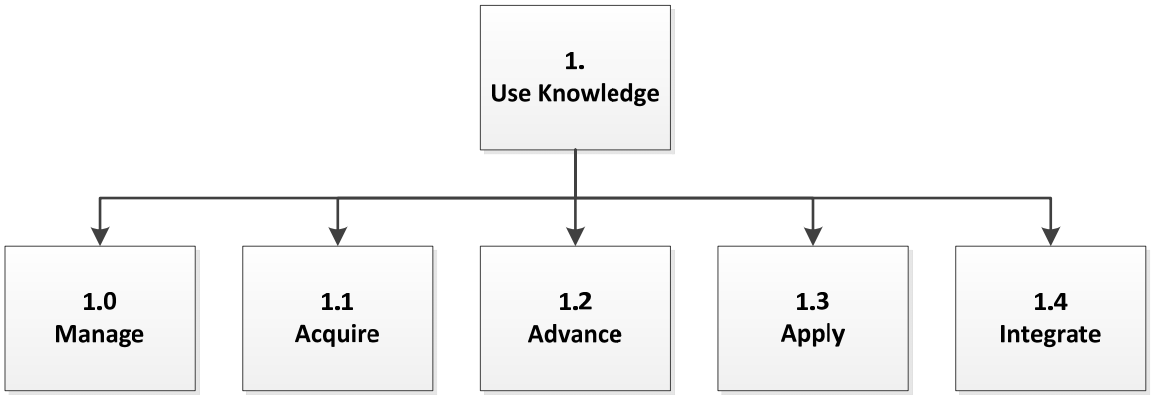

Figure 3. "Use Knowledge" Functional Decomposition

[4] Decision fitness is "illustrated as a chain of steps that describe the appropriate frame for the decision, the creative and doable alternatives that are possible, the meaningfulness and reliability of the information used, the clear values and tradeoffs, the logically correct reasoning, and the commitment to action" (Langford, 2012).

Command and control are functions and are sub-functions of the function “to manage” and these sub-functions can be decomposed as follows:

To command:

- Perform an art of assigning missions
- Provide resources (analyze, prioritize)
- Directing subordinates (guide, set policy and focus the force to accomplish clear objectives
- Analyze risk (identify and assess)

To control:

- Define limits
- Negotiate
- Deal with constraints
- Determine requirements
- Allocate resources
- Report
- Maintain performance monitor, identify and correct deviations from guidance.

Command is different from control and these functions are often performed by different people.

3. Goals of a C2 System

C2 systems exist for the following reasons:

- To provide on-demand or just in time fused intelligences and situational awareness to the combatants.
- To provide rapid turnaround time for collaborative planning
- To provide rapid turnaround time for course of action
- To support agile decision making
- To support collaborative decision making
- To provide information that is sufficiently informed by intelligence, surveillance and reconnaissance (ISR)

Thus, time is of the essence for C2 systems—for information exchange, processing and decision-making—especially for those working in collaboration. Delays (in system processing, communications or human) could result in late system and human response to a dire situation.

B. EVOLUTION OF COMMAND AND OF CONTROL

In understanding command and control, it is pertinent to first look at the revolution of military affairs. Missions today have evolved significantly from traditional military missions as a result of technological advancements, increasing asymmetrical challenges, the move from standalone systems to increasingly interconnected systems (emergence of system of systems ideology) and the move from platform-centric to network-centric warfare. Troops are now well connected in information networks, enabling individuals to operate in a distributed manner in a system of systems, increasing their capability to perform more effectively and in more complex scenarios. With the shift towards network-centric operations, the amount of data and information exchange inevitably increases. However, this paradigm requires the system nodes that are connected in these networks to be able to efficiently and effectively manage, process and exchange information between them.

> Today's missions differ from traditional military missions, not just at the margins, but qualitatively. Today's missions are simultaneously more complex and more dynamic, requiring the collective capabilities and efforts of many organizations in order to succeed. This requirement for assembling a diverse set of capabilities and organizations into an effective coalition is accompanied by shrinking windows of response opportunity. Traditional approaches to C2 are not up to the challenge. Simply stated, they lack the agility required in the 21st century. (Alberts & Hayes, 2006)

With military systems becoming increasingly connected, they become more agile and more able to handle peacetime and wartime scenarios. For example, the configuration of these systems assigned to a mission can be more efficiently rearranged depending on the capabilities of these systems; to work on the next mission as another set of systems without needing to recall/retrieve

them and restructure their communication and data exchange media. This could potentially cut a huge portion of mission preparation time.

> Although the purpose of Command and Control has remained unchanged since the earliest military forces engaged one another, the way we have thought about Command and Control and the means by which the functions of Command and Control have been accomplished have changed significantly over the course of history. These changes have resulted from the coevolution of Command and Control Approaches with technology, the nature of military operations, the capabilities of forces, and the environments in which militaries operate. (Alberts & Hayes, 2006)

C. DISCUSSION OF PROBLEM DUE TO INCREASING RELIANCE ON UNMANNED SYSTEMS

> UAVs were considered exotic toys and not essential tools for victory on the modern battlefield. This all changed as the U.S. demand for surveillance assets soared and its fleet of UAVs expanded by leaps and bounds. (Quincy, Thompson, Moran, Nilsson, & Johnson, 2010)

Unmanned vehicles are now seen less as a completely separate entity within the U.S. Department of Defense and have slowly gained a high level of acceptance and recognition as systems with improving reliability. With use of UAVs increasing from about 1,000 flight hours in 1987 to over 600,000 flight hours in 2008, their presence in combat has grown exponentially.

Unmanned systems are gaining recognition in their fields (military or commercial) for their ability to relieve humans in tedious, repetitive and dangerous tasks. These provide new opportunities to augment the military and as avenues for experimentation. They have been employed by the DoD in air, ground and maritime domains intelligence, surveillance and reconnaissance (ISR) missions, convoy missions, improvised explosive device (IED) detections and mine-clearing.

This increasing use of and reliance on unmanned systems would inevitably lead to an increase in data and information exchange, especially when these unmanned systems operate in a network of systems. There is a need to

manage the increase in data transmission, through stable and uninterrupted information transmission. This means that more resources (such as processing speed and bandwidth) are needed to handle the increase in network data, whilst maintaining the latency rate or delay times of the information exchange and with no compromise to data accuracy and transmission precision (i.e., correct data is sent to and received by the correct sender and recipient respectively).

There is now a need to ensure high reliability of the unmanned systems (in terms of both hardware and software) and their precision performance so that they will be able to replace previously manned systems in performing their missions or complement their operations.

D. PROBLEMS ASSOCIATED WITH LIMITATIONS OF EXISTING SYSTEMS TO DEAL WITH INCREASING NUMBER OF OBJECTS

With the networks of today's systems already saturated with systems communicating and exchanging data with each other, when more objects try to join these networks, existing networks (including their system nodes) are unlikely to be able to handle the load. In addition, with fast advancing technology, system design and requirements would undoubtedly become more demanding and more challenging to achieve as expectations of senior commanders increase. Key problems related to the increasing number of objects introduced into the battlespace include the following:

1. Increasing Complexity and Interconnectedness

Langford (2012) described, "The more ambitious the integration, and the more out of control are the interfaces (i.e., not under change control or management), the more difficult the integration of the new product or service into the existing users' environment and enterprise." Indeed, with more systems (manned and unmanned) added to interoperate as a SoS, complexity in the integration increases as there is a common ontology and set of standards that they will need to conform to, including the use of consistent information assurance methodologies used between interacting systems.

Imposing these requirements on new systems to add to the SoS could be difficult, as they could be commercial-off-the-shelf (COTS) and thus be difficult to change (unless a high cost is incurred) or be OEM (Original Equipment Manufacturer) propriety systems that the OEMs refuse to modify or refuse to sell if their systems are going to be modified after sales. For legacy systems, enforcing standard ontology and standards for them to follow would also be challenging to achieve as these legacy systems are steeped in their own set of integration ontologies, standards and information assurance methodologies. To invoke a change in this would incur time and cost.

Each system may also have its miniscule instabilities, which do not present themselves when these systems operate solo, but when operating together with other systems in a SoS configuration could initiate a chain of events, which could ultimately cause the entire SoS to fail. Thorough study, design and planning of the interfacing systems and understanding of their limitations in terms of data processing capability and transmission bandwidth should be carried out to identify any shortcomings that the individual systems and overall SoS would have in addressing the needs of the stakeholders.

2. Technological Limitations

Today, with rapidly advancing technology and the constant push for excellence in both the military and the commercial market, products are often short of that one characteristic or element that would make it perfect. Similarly, for military systems, including C2 systems, the stakeholder expectations of these systems continue to grow with the system improvements and the technological gap will always exist.

Technology maturity is a constraint on the achievability of future C2 systems. System processing speeds and data storage are limited by the computer processor performance and capacity. Speed of data exchange between systems is constrained by the speed capabilities of existing systems to handle amounts of data larger than these systems have been designed for,

without affecting the relative speed of overall system performance. With the increasing number of objects sharing in the information and communication data bandwidth in the SoS, besides the high speed of transmission, accurate data and precise transmission are also important. Data packages should be sent to and received by intended parties, as they had been sent out by the sending party. On the contrary, data packages should not be sent to or received by unintended parties.

E. GOVERNANCE CHALLENGES

In their report on *Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise*, the (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2009) has highlighted a number of factors that have contributed to the DoD's slow progress in attaining the goal of interoperability. Most importantly, "all combatant commands, military departments, and other defense components need the ability to operate unhindered in cyberspace, the domain does not fall within the purview of any one particular department or component." This results in the lack of an overall systems architecture, lack of a comprehensive interoperability risk analysis, which considers information assurance for net-centric/cyber systems and lack of planning and management of bandwidth and frequency allocation. The acquisition system has been unable to provide timely procurement of net-centric/cyber systems to the warfighter, leaving a disparate set of current and legacy systems in the fleet.

There is also the need for greater cooperation and collaboration between government (including government interagency collaboration), academia, and industry to address these challenges. Including academia and industry early in technology planning for interoperability and future capabilities could cut design and development time wasted for the industry to come up with new capabilities that do not add value to the military in attaining interoperability.

Finally, effective governance of the overall interoperable system of system, when attained, would need to be addressed as this domain currently does not fall under the purview of any single department or component. Roles and responsibilities would have to be properly planned out to avoid conflicts in command and control amongst the combatants in the SoS. Effective governance is made more complex with more systems being introduced into the SoS.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROBLEM DEFINITION

The key problem to address was the establishment and maintenance of interoperability in a target-rich environment.

A. PROBLEM DECOMPOSITION

The problem statement was decomposed into its key elements, “interoperability” and “target-rich environment,” in this section to better understand the issue at hand. Interoperability was discussed in Chapter I and is the ability of systems, units or forces to provide data and information to and accept the same from other systems, units or forces and to use the data and information exchanged to enable these entities to operate together to achieve a common goal. The notions of “systems of systems” and “network-centric warfare” are related to the problem statement as these systems described in the definition of “interoperability” are connected via networks and form systems of systems (SoS), locally and globally. Subsequently, what a ‘target-rich environment’ is and how it would affect interoperability was studied.

1. System of Systems

A paper on Systems-of-Systems by (Maier, 1999) described that:

> Systems-of-systems should be distinguished from large but monolithic systems by the independence of their components, their evolutionary nature, emergent behaviors, and a geographic extent that limits the interaction of their components to information exchange. Within these properties are further subdivisions. For example, a distinction between systems which are organized and managed to express particular functions, and those in which desired behaviors must emerge through voluntary and collaborative interaction. (Maier, 1999)

Five principal characteristics are useful in distinguishing very large and complex but monolithic systems from true system-of-systems. The following characteristics are inherent in a system-of-systems:

1. Operational Independence of the Elements: If the SoS is deconstructed into its sub-systems, the component systems must be able to usefully operate independently. The SoS is composed of independent systems which are useful in their own right.
2. Managerial Independence of the Elements: Although these component systems are able to operate as a SoS when they are integrated together, the sub-systems continue to maintain individual, independent operational existence whilst being a part of the SoS.
3. Evolutionary Development: The system of systems' capability continues to change as more systems are added. As technology and ideas progress, there is no need to redefine the systems of systems, but only the capability of the SoS continue to evolve and change.
4. Emergent Behavior: The SoS performs functions and carries out purposes that do not reside in any component system. These behaviors are emergent properties of the entire system of systems and cannot be localized to any component system. The principal purposes of the systems of systems are fulfilled by these behaviors.
5. Geographic Distribution: The geographic extent of the component systems may be large. Large is a nebulous and relative concept as communication capabilities increase. At a minimum, "large" means that the components can readily exchange only information and not substantial quantities of mass or energy.

To attain interoperability, the components of command and control are needed to complement and regulate the system of systems. The SoS's emergent and evolutionary characteristics as more component systems are added could be both beneficial but disadvantageous depending on the management of these component systems (they are operationally and managerially independent). Trust is an important interfacing component that these systems have to earn and maintain for them to be part of the SoS. If a system breaches the trust of another system through sending non-standard or corrupted messages, the connecting system could choose to drop this system's connection.

2. Network-Centric Warfare

Network-centric warfare (NCW) is an emerging theory of war in the Information Age. It is also a concept that, at the highest level, constitutes the military's response to the Information Age. The term

> network-centric warfare broadly describes the combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even a partially networked force can employ to create a decisive warfighting advantage. (Department of Defense, Office of Force Transformation, 2005)

The backbone of interoperability is the notion of network-centric warfare across the spectrum of conflict, from peace, to crisis, to war. The network is the information technology in the SoS architecture and thus the enabler for the conduct of warfare in a networked environment. "Networked" is one of the seven attributes, identified by the Joint Operations Concepts[5] (JOpsC) that the future Joint Force must possess, the others being "fully integrated," "expeditionary," "decentralized," "adaptable," "decision superiority" and "lethality." According to the JOpsC, "networked describes a Joint Force that is linked and synchronized in time and purpose." Having the units linked via networks promotes positive network externality[6] through enabling them to more efficiently communicate, share a common operating picture and achieve the desired end-state. The networked joint force would be better able to achieve beyond the organic capabilities of individual units to include fire support, sustainment and information. The network can include interagency, multinational allies, academia and industries. Planning of the networks is important to ensure optimal exchange and propagation of data through them. Negative network externalities such as having more systems joining the network than the network can handle to operate optimally could cause the network to meltdown.

With the heavy reliance on technology, increasing collaborations between

[5] The Joint Operations Concepts is "an overarching definition of how the future Joint Force will operate across the entire range of military operations. It is the unifying framework for developing subordinate joint operating concepts, joint functional concepts, enabling concepts, and integrated capabilities." (Department of Defense, 2003).

[6] Network externality has been defined as a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes. (Liebowitz & Margolis, n.d.).

systems and military forces and the unchanging need for rapid decision-making, network-centric warfare is a concept that is at the very heart of the military operations of today.

3. Target-Rich Environment

With the increasing numbers of unmanned systems employed in the military and the increasing reliance on them, the systems entwined in the future battlespace will have to combat the potentially vast quantities of data to manage, harvest and propagate within the SoS. This increase in data is a result of the large number of targets present in the systems' tactical pictures (including own-force units in their vicinity) and the data exchange between the large numbers of own-force units in contributing to the overall situational awareness of the SoS. A target-rich environment—many own-force units in an environment with many other systems—brings with it communication and data management challenges. In a SoS, systems must be able to handle the data load and ensure the data exchanges are accurate and precise.

> As the number of fielded systems grows, communications planners face challenges such as communication link security, radio frequency spectrum availability, deconfliction of frequencies and bandwidth, network infrastructure, and link ranges. Intelligent means of data parsing is needed to enable TPED (Tasking, Production, Exploitation, and Dissemination) and counter communication challenges. (Department of Defense, 2011)

TPED is required to convert large amounts of sensor data into a common understanding of the environment. With more collaboration between inter-government agencies and between allies, these communication challenges will only worsen and result in the limited communication between collaborating contingents or those limited information exchange if interoperability is required.

Alongside communication challenges, having more targets inside the operational area of the SoS strains the management of the data within each system and the data exchanged, and the management of large number of systems being deployed. Deployment of vast quantities of systems into theater

and keeping them under command and control is challenging. These systems could be better managed through distributed command and control, in which key entities are selected as the main “command posts” empowered to control the lower entities within their local control perimeter. If not done properly, information or commands that are to be propagated to selected nodes will not reach these nodes or will be received by nodes not supposed to receive them.

In planning for interoperability in a SoS configuration, one should gather information on the purpose, data capacity and processing speeds of the systems that is or will be part of the SoS. These system limitations restrict the type and size of the data that will be exchanged and received by these systems. Identifying the roles that these systems will play within the SoS (e.g., as relay nodes or intelligence-gathering) can help to frame the data package that is being received and/or sent by them.

B. BOUNDARIES & BOUNDARY CONDITIONS

> A condition is the circumstances that encompass an object; the factors that affect the manner and ways in which the object interacts; the situation in which the object operates; or the terms under which an object behaves. An object is influenced by its sensitivities to conditions. (Langford, 2012)

To help scope and bound the problem addressed in this thesis, the boundaries (physical, functional and behavioral) of the problem and the conditions in which these boundaries will be affected is discussed in this section.

1. Physical Boundaries

a. Geographical Location of the SoS Deployment

The geographical location of SoS deployment affects the amount of systems/units deployed, the amount of other non-own-force units that will be detected and shared amongst own force units as the common situational picture and tempo of battle. If the SoS is deployed into enemy territory, implications such as rapid and large amounts of data exchange and jamming of the SoS

communications will have to be taken care of. Interoperability requirements would be different depending on which spectrum (peace or war) of military operations the units in the SoS have to combat, which is affected by where they are deployed.

b. Operating Range of Systems

The operating range of the component systems' communications equipment is a limiting factor which will result in a break in the data transmission (if any) when one end of the system moves outside the communications operating range. Operating range is also limited when integrating with ground systems that may face challenges of detecting other collaborating systems operating at low altitudes (including other ground systems), additional systems such as unmanned aerial vehicles could act as relay nodes to pass message to and from these ground systems, thereby providing an extension to the operating range of these systems.

2. Functional Boundaries

a. To Communicate

Communication is a key function for the systems within the SoS network to enable them to interoperate/collaborate with each other. According to Dictionary.com, communication is the imparting or interchange of thoughts, opinions, or information by speech, writing, or signs (n.d.). In the context of this thesis, communication is the interchange or exchange of data, or information via network links such as local area networks (LAN) and wide area networks (WAN). These network links include the military data link radio networks using military data link standards such as Link 4, Link 11, Link 16, Link 22 and the variable message format (VMF) (Sturdy, 2004). The concept of NCW can only be achieved through communication within a SoS, without which, interoperability amongst the component systems cannot be achieved.

b. To Command

As defined in Chapter I, “to command” is to perform the art of assigning missions; providing resources (analyze and prioritize); directing subordinates (guiding, setting policy and focusing the force to accomplish clear objectives); and analyzing risk (identifying and assessing). The key focus areas of command in this paper was the authority that sets the policies and provides guidance to focus the force to accomplish clear objectives through mission objectives and establishing and giving them a clear concept of operations (CONOPS) for these missions. In addition, the authorities in command will have to be clear in their requirements for the SoS architecture to facilitate interoperability between these systems, and know the roles that the component systems play in the overall system and their placements in the overall hierarchy of systems.

c. To Control

As defined in Chapter I, “to control” defined limits; negotiated; dealt with constraints; determined requirements; allocated resources; reported; and maintained performance (monitored, identified and corrected deviations from guidance). Control includes the control of complex systems within the SoS which requires intelligence, communications and a mechanism for exercising authority (or ‘to command’). The more entities in the system, the “more critical, complex, and potentially vulnerable the central (the authority in-charge) become.” There is the question of centralized or distributed control over these elements in the network—too little distribution could overwhelm the controlling central whilst overly-distributed control could cause conflict, confusion and breakdown of the overall network. “Too much distribution of authority without distributed intelligence (whether human or machine) and there can be unresolvable conflict, confusion, and breakdown” (Rechtin, 1991).

d. To Propagate Information

Information propagation can be seen as a parallel or a desired end-state to communication. Propagation of information is required for the systems within the SoS to share its knowledge of the situational picture with the other system nodes that require them or are required to relay them further. If the system nodes designated to pass the information to its children nodes do not propagate the data/information as required or designed for the SoS network architecture, these children system nodes will not receive these data/information, and thus lose out on the common situational picture.

e. To Process Information

Individual system nodes in the network of SoS have to process the information that is sent to them, this includes filtering of unnecessary or unwanted data besides using them to result in an action at the system levels. Information to be propagated to adjoining nodes will also have to be processed or restructured to meet the interface specifications of the receiving node. In performing this function, the system node will have to ensure that the data or information received or sent are interpreted or parsed accurately, respectively. Inaccurate interpretation or parsing of data/information could lead to data corruption and this corruption could be propagated to the rest of the interoperating systems, or be filtered away by the first receiving party. This miscommunication could be controlled via the data filter processing of the receiving system node.

3. Behavioral Boundaries

a. SoS Emergence

Emergence is defined by Langford (2012) as any effect that produces a change in intrinsic properties, traits or attributes that result by

combining objects through the interactions of objects with EMMI. Emergence is due to the traits of an object or objects, process or processes. Emergent behavior is resulted when:

> The system performs functions and carries out purposes that do not reside in any component system. These behaviors are emergent properties of the entire system-of-systems and cannot be localized to any component system. The principal purposes of the systems-of-systems are fulfilled by these behaviors. (Maier, 1999)

Emergent properties may be beneficial, e.g., if the users adapt the resultant system to support tasks that the SoS architect never intended; or may be harmful, e.g., if safety requirements are undermined. (Johnson, 2012) Care will need to be taken during system architecture design to ensure there is sufficient control over the system behavior (through clear requirements and traceability of system design to these requirements) to avoid negative emergence and avoid breach of safety requirements.

It may not be possible to prevent all causes of negative emergence. Measures may only be plausible when negative emergence occurs and its cause identified. In situations such as this, the problem may be correctable; otherwise, the operators of the systems involved could be warned to prevent action that would “activate” or propagate the emergence.

b. Governance of Systems

How the component systems contribute to the SoS, where they exist in the SoS architecture and the interfaces between these systems should be considered in the overall SoS risk assessment. Standards limiting the component systems’ and the interfacing specifications should be established and propagated to the component systems as a form of governance to prevent the occurrence of unexpected emergence behavior of the combined system.

In addition, when systems interoperate or collaborate to work towards a common goal or mission, they may run into a situation in which it is no longer clear who has the overall command and control of these systems, which

form part of a bigger system-of-systems. This situation is what would happen when the integration of SoS entities are comprised of international allies—the aggregated forces operating on the same level of command, which could result in conflicts. The hierarchical structure of the SoS need to be well planned out.

c. Data/Information Propagation

Data/information propagation refers to the distribution of data/information between system nodes in the SoS. Efficiency of data/information distribution depends on the system network topology[7] (e.g., bus, star, ring or mesh) and communication structure (i.e., determining which systems are pure receivers, pure transmitters and receiver/transmitters). A network's topology affects its capabilities. Which topology is deployed for a SoS will impact the type of equipment the network needs, capabilities of the equipment, and the growth of network and the way in which the network is managed (Hsieh, n.d.). The communication structure will constrain how the data/information can be propagated in the network, e.g., system A, that is not supposed to have visibility or connection to system B, will not receive or send any information directly to system B. Changes to the network topology and communication structure would definitely influence the effectiveness of the mission carried out by the SoS.

C. LIMITATIONS AND CONSTRAINTS

Limitations describe the extremes of operability of an entity at its boundaries (the physical extend of an entity); limitations are given by the domain of the problem and are conditions of boundaries, and once imposed they are immutable. Constraints on the other hand, are a structural property of the solution. Constraints are the results of boundary conditions. Constraints are conditions of allocations that once established are changeable, however vicissitudinous. Constraints are flexible within the overall limitations set (Langford, 2012).

[7] A network topology refers to the arrangement or physical layout of computers, cables, and other components on the network (Hsieh, n.d.).

Identifying the limitations and constraints of the solution space to address the problem of establishing and maintaining interoperability in a target-rich environment would help to scope the problem and discard solutions that will affect these limitations and constraints.

1. Limitations

a. Operational Space

This refers to the area of operations in which the SoS will carry out its mission. The operational space will limit the extent of the network growth and act as the limiting operating range of the communication linkages between systems.

b. Control

"Control" by definition defines limits and by its action in the military context, imposes a limitation on the units/forces/systems under the "controller" to act on their own free will. Control refers to both the structure within which how the units/forces/systems are specified to perform (such as network architecture and hierarchical structure) and the control that the human operators set on the computer systems (e.g., manual, semi-autonomous and fully autonomous).

> Virtually all large complex systems and the organizations that build and operate them are regulated… A well-crafted regulation reduces uncertainty, provides standards, and protects suppliers and consumers against rapacious competitors. Poorly crafted regulation can do severe damage, overburdening and disrupting parts of the economic system. (Rechtin, 1991)

In the context of military C2 systems, poorly crafted regulations can result in loose control over the component systems and result in overburdening and disruption in various parts in the SoS.

c. Component System Performance

The performance of the overall SoS is limited by the performance of the individual component systems that it is made up of. If a component system is

not able to update its system database at the same speed, if not faster, as the data/information is being received it its interface, data overflow could result. The component system would also be unable to store data/information larger than its total database storage size.

2. Constraints

a. Command and Control (C2)

C2 constraints the boundaries within which the systems in the SoS function. These systems, when not within the network of SoS, are able to function without the influence of the SoS. However, when systems join the SoS to carry out missions, they are required to adhere to the interfacing (in terms of data packet formatting) and communication speed restrictions of the SoS.

b. Policies

A set of policies are principles, rules and guidelines formulated or adopted by an organization to reach its long-term goals and typically published in a booklet or other form that is widely accessible (policies and procedures, n.d.). Herein, policies refer to the principles, rules and guidelines that the commanders set and the human operators adhere by in carrying out their duties. Policies are key in keeping operations in control, especially in a configuration of SoS with numerous systems connected and communicating in an environment with large numbers of targets. In the conduct of missions, rules and guidelines could be bent in the process of achieving the ultimate goal of the mission.

D. SCOPE

The scope of this thesis was to identify the key factors necessary in a C2 system architecture to satisfy the needs for a future C2 system so as to establish and maintain interoperability in a target rich environment. It was recognized that it was not possible to specify every factor needed for interoperability between systems to take place. However, key factors that could improve the effectiveness

and efficiency in the establishment and maintainability of intersystem interoperability in a target-rich environment were described in Chapter IV.

E. PROCESS DECOMPOSITION

> A process can be articulated as a systematic pattern, a coordinated set of procedures, tasks, activities, or acts that result from the conversion of inputs into outputs. Process is the amalgamation of activities and tools that combine ideas… From an integration perspective, processes guide the work. (Langford, 2012)

Process decomposition was used to identify the objective and subjective causalities that are relevant to the project, within the framework of integration.

Key processes needed to address the problem of systems interoperability within a target-rich environment were identified using process decomposition and are listed as follows:

1. Develop & Maintain Network Architecture
    - 1.1. Record and keep track of system interactions
    - 1.2. Use common/open architecture
2. Develop & Maintain C2 hierarchy
    - 2.1. Develop clear system reporting structure at higher system levels & propagate hierarchical report down accordingly
    - 2.2. Assign ownership of sub-SoS/network systems
3. Use common ontology within SoS
4. Maintain information security
    - 4.1. Plan & implement hierarchical Information Assurance (IA) requirements
    - 4.2. Develop & implement security policies
5. Perform system integration
    - 5.1. Upgrade legacy systems
    - 5.2. Impose relevant requirements on new systems
    - 5.3. Develop (optional) software patch for ease of integration
    - 5.4. Perform & maintain system-to-system connection / coupling cohesion
    - 5.5. Perform integration testing

6. Maintain system stability

   6.1. Maintain local system stability

   6.2. Maintain global system stability (even in situation of large numbers in system)

   6.3. Plan for high system reliability and maintainability

   6.4. Plan for operator training

IV. DEVELOPMENT OF SOLUTION

A. NETWORK CONTROL THEORY

Management of a large number of systems, which are interconnected based on their functionalities, capabilities and sub-mission allocations, require some form of control mechanism. This mechanism in the engineering discipline takes the form of control architectures. For large-scale systems, three possible control architectures are shown in Figure 4.

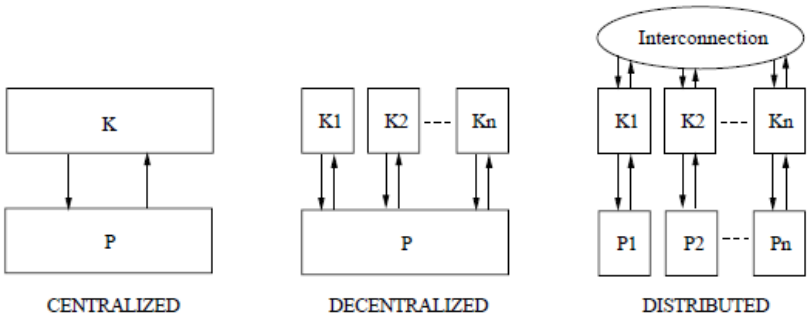

Figure 4. Architectures for Centralized, Decentralized and Distributed Control Architectures (From Jin, 2007)

Distributed control architecture is most suited for the control of multiple decoupled subsystems $\{P_1, P_2, \ldots, P_n\}$, with each subsystem equipped with a local controller. Interconnection exists amongst these controllers so that information can be shared and exchanged and interaction can result between these component systems. Thus, for a network-centric system of multi-agent systems, cooperative and coordinated control of a distributed control structure is most suitable.

A typical diagram for a networked control system (NCS) depicting sub-processes occurring within a subsystem was illustrated in Figure 5. Based on the structure of the NCS, it can be observed that due to the following ideal conditions desired in a network architecture, conventional control theory is not sufficient (Jin, 2007):

- Infinite bandwidth: The communication channel can only transmit data with certain precision under the constraint of limited bandwidth. Quantization and distortion must be considered for system design and analysis.
- Reliable connections: Sampled signals are transmitted in data packages that suffer from reliability issues such as unpredictable transmission delays and random packet drops
- Static structure: For networked multi-agent systems, dynamic routing and ad-hoc connectivity of modern communication networks makes the interaction topology time-variant and the coupling amongst agents may change with time.

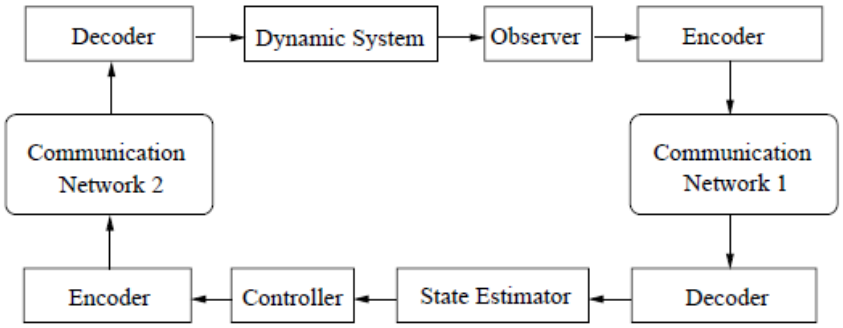

Figure 5. Diagram of a Typical Networked Control System (From Jin, 2007)

Nonetheless, in addition to these considerations, military networks are also affected by the increasing number of systems joining in the SoS networks (due to increasing reliance of unmanned systems and introduction of new systems to augment their warfighting power) and the number of targets in the environment. Connection, coupling and cohesion between these component systems form the basis of interoperability between them.

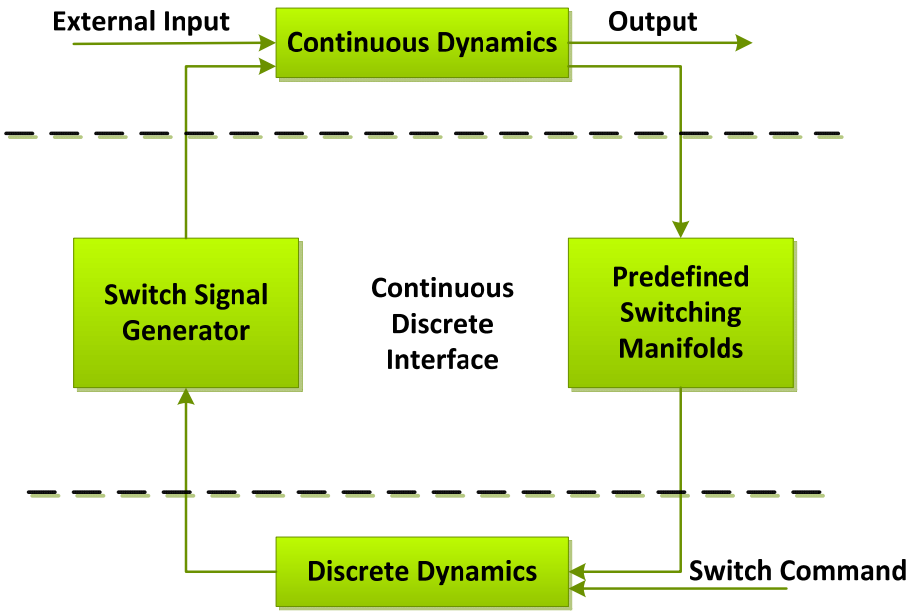

Figure 6. Block Diagram Model of An Autonomous Switching Hybrid System (From Ding, 2009)

According to Ding (2009), hybrid systems were described as:

> [s]ystems that are controlled by discrete events in the higher level, while their dynamical behaviors are governed by continuous dynamical laws in the lower levels… discrete events in the higher level dictate the continuous dynamical behavior of the system in the lower level.

Hybrid system control problems occur in various situations, including those where a control module has to switch its attention among a number of subsystems, interact with them and achieve formation and coverage control of networked systems. Hybrid systems can be modeled using block diagrams as shown in Figure 6. Such block diagrams can be related with interconnected system nodes with discrete events occurring within and between individual nodes, but there are also continuous dynamics occurring outside the systems. This concept was applied to the study of the impact of the number of system nodes within the SoS and the amount of information being shared or exchanged amongst these nodes.

B. APPROACH AND METHOD

To establish and maintain interoperability in a target-rich environment, a systems engineering top-down approach was used to break down the problem space, described in Chapter II, to identify solutions to address these component problems. These solutions are recommendations, which may not apply to all types of system of systems configurations. The recommendations provide a set of guidelines in the development of a C2 SoS architecture.

A pilot study of a network architecture simulating multiple system nodes using the general hybrid system model described by Ding (2009) was conducted. The study explored the influence of the quantity of system nodes in a SoS network, the amount of data/information being passed between the system nodes and how effective (in terms of timeliness) the system nodes are in receiving up-to-date information.

An assessment of the factors required to achieve and maintain interoperability in a target-rich environment will first be discussed in Chapter V. Following which, an ExtendSim model was developed to study the effects of tolerable delays in data/information propagation throughout a multi-node system or system of systems linked together in a network configuration. The results obtained from the model were then discussed.

C. PRINCIPLES

A principle is a means of organizing thoughts to articulate a pattern of behavior that frames or structures action; it represents both the content and concepts that enable us to classify and interpret a situation in terms of previous situations.[8]

Systems integration is not a small task, especially at the scale of an air-defense system (Figure 2.).

[8] A situation is a sequence of events where an event describes an activity that relates an input EMMI to an output EMMI through causal mechanism (Langford, 2012).

> "Application of best practices, or the systems engineering and management skills, products, and services (perfect or not so perfect) embody the key principles of systems integration." Examining these principles (that are evident in one or more case studies) exposes the actions and circumstances that have major influence on the outcomes of system integration." (Langford, 2012)

Some of the following principles proposed by Langford (2012) provided guidance to the development of the solutions described in Chapters V to VII:

- **Principle 1: The Principle of Alignment.** Alignment of strategies for the business enterprise, the key stakeholders and the project results in better outcomes for product or service development.
- **Principle 2: The Principle of Partitioning.** Partitioning of objects can create tractable problems to solve if, and only if, boundary contiguity is achieved.
- **Principle 3: The Principle of Induction.** Inductive reasoning should guide integration management and recursive thinking.
- **Principle 4: The Principle of Limitation.** Integration is only as good as architecture captures stakeholder requirements.
- **Principle 5: The Principle of Forethought.** Integration is a primary, key activity, not an afterthought considered as the result of development.
- **Principle 6: The Principle of Planning.** Integration planning is predicated on pattern scheduling (lowest impact on budget), network scheduling (determinable impact on budget) and ad hoc scheduling (undetermined impact on budget).
- **Principle 7: The Principle of Loss.** When two objects are integrated, both objects give up some measure of autonomous behavior.

These principles could also be used to guide a system architect or integrator in the planning, design and development of any system.

D. HEURISTICS

Lists of heuristic ranging from multitask heuristics, scoping and planning heuristics, and aggregating heuristics are detailed in Maier and Rechtin's, The Art of Systems Architecting (2009). However, it is impossible to identify all heuristics used in the problem and solution formulation of this thesis.

Nonetheless, the following heuristics describe some of the general problem solving and discovery processes employed in architecting this thesis and the network models studied:

- Relationships among the elements are what give systems their added value.
- In general, each system level provides a context for the level(s) below:
    - Leave the specialties to the specialist. The level of detail required by the architect is only to the depth of an element or component critical to the system as a whole. But the architect must have access to that level and know, or be informed, about is criticality and status.
    - Complex systems will develop and evolve within an architecture much more rapidly if there are stable intermediate forms than if there are not.
- No complex system can be optimum to all parties concerned, nor all functions optimized.
- Sometimes, but not always, the best way to solve a difficult problem is to expand the problem, itself.
- Group elements that are strongly related to each other, separate elements that are unrelated.
- Choose a configuration with minimal communications between the subsystems:
    - Choose the elements so that they are as independent as possible; that is elements with low external complexity (low coupling) and high internal complexity (high cohesion).
    - Choose a configuration in which local activity is high speed and global activity is slow change.

V. A FUTURE COMMAND AND CONTROL SYSTEM

A. FUTURE COMMAND AND CONTROL

1. A Science of Command and Control

The increasing complexity of military combat systems and the ever-changing military situation in the world today bring about uncertainties in the nature of future combat and thus a higher demand for flexibility and adaptability of command and control systems. This requires informational advantage and an accurate situational awareness of the battlespace, achievable through effective integration of heterogeneous sensors, arms and communication systems.

Skyttner (2005) described a science of command and control through three various perspectives, namely: the General Living Systems (GLS) perspective, cybernetic perspective and communication and information perspective, which future C2 systems can be built based on. In thinking of C2 systems, this science of C2 could be used to abstract the component systems and data and information exchange to facilitate the design and development process of C2 architectures.

B. NEED FOR INTEROPERABILITY

> We must achieve: fundamentally joint, network-centric, distributed forces, capable of rapid decision superiority and massed effects across the battlespace. Realising these capabilities will require transforming our people, processes and military forces. (Rumsfeld, 2003)

Possessing the capability to operate in a network-centric configuration has seen positive results in the battlefield. With NCW, geographically dispersed forces are able to achieve strategic, operational and tactical advantages through attainment of a high level of shared situational awareness. This interlinking of systems (people, platforms, weapons, sensors and decision aids) into a single network “creates a whole that is greater than the sum of its parts.” Networked forces become able to operate with increased speed and synchronization and

are capable of achieving massed effects, oftentimes, without the physical massing of forces required in the past (Department of Defense, Office of Force Transformation, 2005).

1. Levels of Interoperability

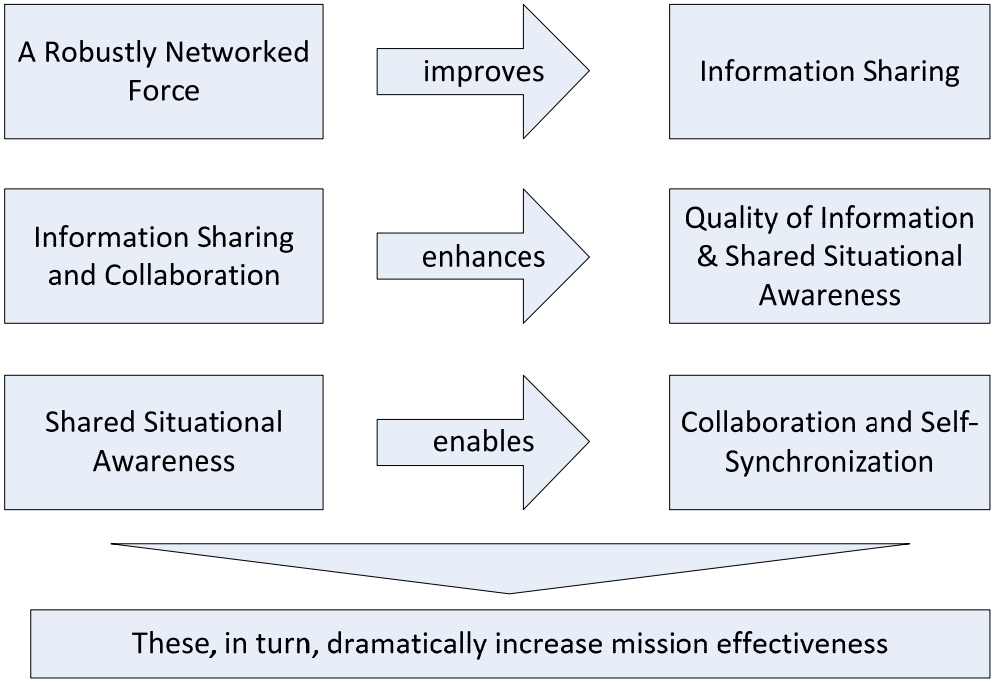

Figure 7. Network-Centric Warfare Tenets
(From Alberts & Hayes, 2003)

Alberts and Hayes (2003) described the basic tenets of NCW as illustrated in Figure 7.

> The degree to which forces are interoperable directly affects their ability to conduct network-centric operations. Interoperability must be present in each of the four domains: physical, information, cognitive and social.

The level of interoperability between systems can also be evaluated through the relationships between these systems based on their connectivity, coupling and cohesion. Connectivity[9] between systems (force entities, as well as

[9] "Connectivity is the physical connection between objects. Connection is established by an interaction of one object with another through EMMI" (Langford, 2012).

other entities that the force needs to work or collaborate with) is the first step to interoperability—a physical connection between them is required for data and information transmission. Cohesion and coupling are direct indicators of interaction as they are defined as measurable concepts, rather than specific measures. Cohesion is the characterization of the measure of binding between two objects through their interaction(s). The strength or degree of interaction means that two objects can be coupled under various conditions in which their interactions can change each other. Coupling is the degree of dependency between objects or processes (Langford, 2012).

2. NCW Maturity Model

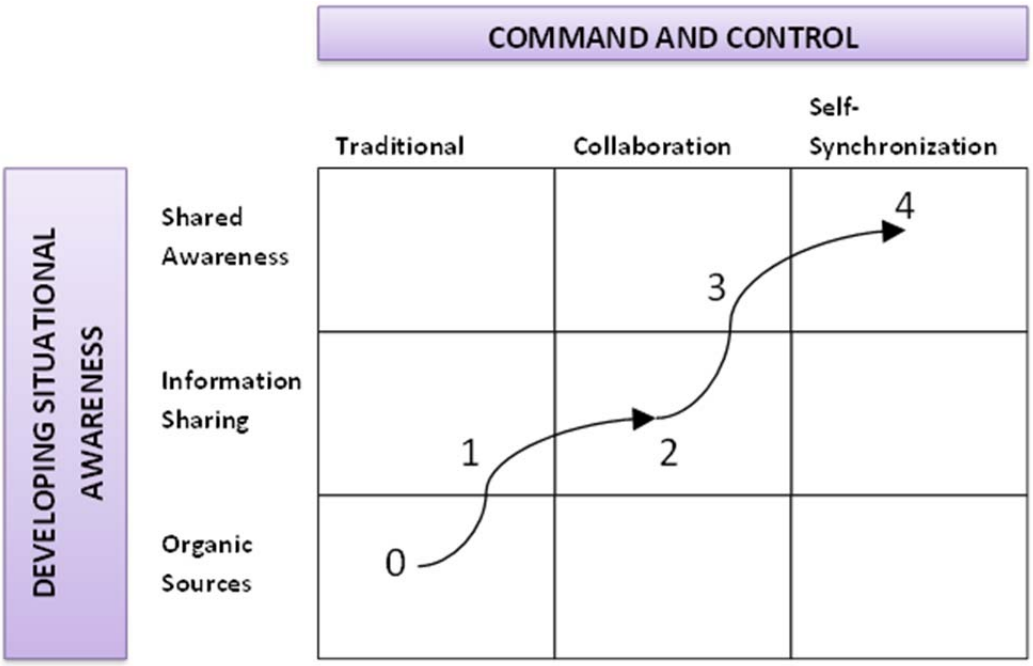

Figure 8. NCW Maturity Model (From Alberts & Hayes, 2003)

The network-centric maturity model, depicted in Figure 8. , defines five levels of maturity and a hypothesized migration path for the implementation of network-centric capabilities in an organization (Alberts & Hayes, 2003). In a pure platform-centric, stove-piped world, sensors are “owned” by the platforms and the information available to those on a given platform only comes from these

“organic” sensors. Thus, situation awareness is only developed from organic sources. Level 0, the baseline, is defined as operations that employ traditional command and control processes (e.g., centralized planning) with information created solely from organic sources. As the level progresses, the maturity of the situational awareness becomes more network-centric.

However, to arrive at the end-goal of “joint, network-centric, distributed forces capable of rapid decision superiority,” the systems in these distributed forces must first possess the capability to connect to and interact with other systems in the network. The challenge in interlinking these systems is not isolated to the technicalities of the systems integration, such as developing interfaces for the systems to be integrated and taking into consideration the data/information exchange limitations in terms of data rate and size. It is also important to ensure that the stability and security of the integrated system are not compromised. These elements and other factors important in the achievement of interoperability are discussed in the next section.

C. KEY FACTORS REQUIRED FOR INTEROPERABILITY

Interoperability, as described in Chapter I, is the ability of systems, units or forces to provide data and information to and accept the same from other systems, units or forces, and to use the data and information so exchanged to enable these entities to operate together to achieve a common goal.

There is no one formula to achieving interoperability. The composition of the systems, operating environment, operators, commanders would be different between different types of SoS. A different set of requirements for each SoS would drive a different design and architecture for the SoS. Nonetheless, through breaking down the problem of “establishment and maintenance of interoperability in a target-rich environment” and identifying the boundaries, limits and constraints, key processes required to address this problem of interoperability

had been identified in Chapter III. In this section, these processes will be presented in detail to illustrate why they are important for a successful SoS interoperability.

1. Network Architecture

Network architecture was not studied in detail in this thesis, but nonetheless has a large impact on the efficiency (speed of data/information propagation) and effectiveness (percentage of systems receiving data/information intended for them) of the system of systems. Today, systems are increasingly being connected and integrated to achieve a higher goal or capability. In dealing with a system of several heterogeneous systems, a well-planned and implemented network architecture needs to be in place to prevent negative network externalities and thereby facilitate smooth system operations.

a. System Interactions

Various network topologies have been used in LAN and WAN designs, some of which include bus, ring, star and hybrid networks. There are advantages and disadvantages to each type of topology as described by Pawar (2008) and the Florida Center for Instructional Technology (2012). Dekker (2005) also explored networks generated using the method of Scale-Free Networks introduced by Kawachi, Murata, Yoshii and Kakazu (2004), in which the topology of a network can be altered to match the connectivity requirements of the component systems without altering the number of links.

Network architectures should be chosen on the interaction requirements of the component systems in a SoS. In dealing with the interactions between a large quantity of systems, a star-bus topology (Figure 9.) which combines characteristics of linear bus and star topologies can be used (Hsieh, 2012). This type of topology minimizes failure of the entire network, as the breakdown of a child subsystem that is not a parent to other subsystems would not affect the rest of the network. If a hub (a system connected to both parent

and child-type systems) fails, all child systems connected to that hub will be unable to communicate with the rest of the network and vice versa.

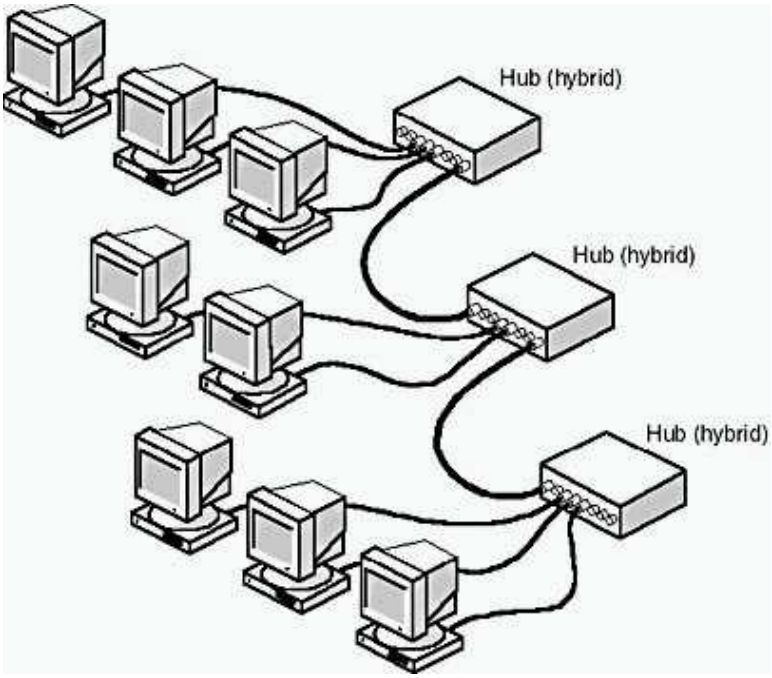

Figure 9. Hybrid Star-Bus Network Topology (From Hsieh, 2012)

A combination of top-down and bottom-up design methodology can be used to map the network architecture of participating component systems in a SoS. Operational capabilities (in terms of storage, processing and functionalities) and available interfacing connections of participating systems should be noted and considered in the SoS network architecture design. With clear SoS goals and mission objectives, these mission requirements can be decomposed into individual processes which can be matched against sub-system clusters able to meet these objectives. Through iterative matching and modifying the links between systems (taking into consideration the processing/storage capacity discrepancies and available connection mediums), network connections could be mapped out.

For SoS types involving multiple domain platforms, i.e., land, air and sea assets, care must also be taken to ensure that the network architecture is able to work within the limits of the component systems' operating ranges depending on their geographical deployments. For example, the operational connectivity of an asset working at a distance outside line-of-sight range of land/sea platforms could be extended through deployment of air platforms (such as UAVs) to act as interim connecting sub-systems to extend the SoS network's geographical operating range to that asset.

b. Use of Common/Open Architecture

In network infrastructure, the term 'open architecture' refers to the practice of using virtually any combination of standards-compliant components in the design of the network. (Hitachi Cable Manchester, 2012) Analogous to the ease of communications between individuals who speak the same language instead of different languages, the use of a common architecture such as open architecture could potentially ease the systems integration process.

To meet Chief of Naval Operations (CNO) of the U.S. Navy, ADM Roughhead's priorities to exploit cutting-edge technology and identify the way ahead for the U.S. Navy, the Naval Open Architecture (OA) vision was to:

"Transform our organization and culture and align our resources to adopt and institutionalize open architecture principles and processes throughout the naval community in order to deliver more warfighting capabilities to counter current and future threats."

The desired state of the military include being able to leverage on the information-centric, common platforms that facilitate collaboration between joint forces and international partners, and having new systems that not only addresses the current needs but also have the flexibility and extensibility to handle the future challenges of the battlefield. There are several challenges that need to be overcome in order to achieve this desired technical state. Steady or declining defense budgets drive the shift towards enterprise architecture enabling

software modularity and reuse to reduce both cost and risk in procurement, maintenance and system upgrades. Contracts and incentives must reshape business models in dealing with industrial partners to break away from traditional, closed platform style of procurement. Open architecture would provide the means for the military to meet such challenges.

> Naval Open Architecture is the confluence of business and technical practices yielding modular, interoperable systems that adhere to open standards with published interfaces. This approach significantly increases opportunities for innovation and competition, enables reuse of components, facilitates rapid technology insertion, and reduces maintenance constraints. OA delivers increased warfighting capabilities in a shorter time at reduced cost. This initiative is a key enabler and pillar of the Department of Defense's (DoD) focus on joint architectures and evolutionary acquisition.
>
> By adopting OA principles throughout the Naval enterprise today, we can build modular, affordable, future National Security Systems designed to meet the future needs of our warfighters. These systems will also be able to readily incorporate insertion of new technologies from a broad range of industry partners. (Office of the Chief of Naval Operations Staff [OPNAV], 2008)

The Office of Naval Operations Staff, Warfare Requirements and Programs (N6/N7) identified the following five principles to guide their efforts towards achieving the Naval OA Vision:

1. Encourage competition and collaboration through development of alternative solutions and sources.
2. Build modular designs and disclose data to permit evolutionary designs, technology insertion, competitive innovation and alternative competitive approaches from multiple qualified sources.
3. Build interoperable joint warfighting applications and ensure secure information exchange using common services (e.g., common time reference), common warfighting applications (e.g., track manager) and information assurance as intrinsic design elements.
4. Identify or develop reusable application software selected through open competition of "best of breed" candidates, reviewed by subject matter expert peers and based on data-driven analysis and experimentation to meet operational requirements.
5. Ensure life cycle affordability including system design, development, delivery, and support while mitigating Commercial off

the Shelf obsolescence by exploiting the Rapid Capability Insertion Process / Advanced Processor Build methodology.

The execution of the naval open architecture has proven to be successful and effective, relying on substantive and concerted contributions of analysis, thought leadership and work by key stakeholders (OPNAV, 2008).

In the Open Architecture Technical Principles and Guidelines compiled by IBM, open architecture is described to be “a pattern of nonfunctional requirements (NFRs) that contribute to the ability to create, deploy and manage OA systems” (Nelson, 2008). With the increasing use of open standards in both COTS and open-sourced software, the visibility of component-based, interchangeable software for complex systems is increased and OA is viable.

The use of open architecture has yielded positive results:

- Rapid adoption of technology.
- Easier test and integration.
- Rapid improvement in technology capability and performance.
- Reduced life cycle cost due to increased competition, easier maintenance and upgrades, broader knowledge base and greater exploitation of reusability.

Nonetheless, for open architecture to be embraced by the military community, industrial partners/contracts would also have a part to play in incorporating open architectural concepts into their products and services. Conversely, the military procurement department or agencies could also set the use of open architecture as a requirement for the systems, platforms or services that they wish to procure from these contractors.

2. Command and Control (C2)

a. C2 Systems

C2 systems are important in orchestrating groups of systems/platforms as they facilitate the information exchange, processing and decision-making process of these systems/platforms. With increasing reliance on

unmanned systems, increasing deployment of highly complex systems and increasing number of targets in the battlefields of today, C2 systems take on a heavier responsibility in providing on-demand or just-in-time situational pictures to the combatants.

To manage this, C2 systems also become more interconnected, and thus complicated. Care should be taken to control the C2 evolutionary development such that the system, both locally and as a global system of systems, continue to remain in their metastable, if not stable state.

Other challenges of command and control systems include the "difficulty of accomplishing changes in established networks," "the continuing growth of most communication networks," and the "need to respond promptly and reliably during crises" for real-time intelligence systems and the critical interface between the systems and the commanders (Rechtin, 1991). Planning and designing for the potential occurrence of these challenges during the design and development phases of the SoS network architecture would help prepare the SoS stakeholders for the change.

For C2 systems operated with humans-in-the-loop, key decisions such as fire-commands are usually still left to the operator to decide and give the go ahead. However, humans are not as adept at processing large amounts of data/information within a short time frame as the machines, although humans are better able to make sense out of a limited set of data/information than machines. To cater for human decisions and responses, pre-processing data/information by the machines and controlling the amount and type of information to be presented to the human would help reduce the mental stress that could be put on the human when large amounts of information is presented to him/her.

b. C2 Hierarchy

Despite variations in the definition of "Command and Control," "command" was consistently identified with the authority which takes charge of the decision-making, and sets policies and provides guidance to help the

combatants accomplish their mission goals with clear instructions (mission objectives) and concept of operations. Command can also be considered as a subset of control, in which commanders determine how the forces are to be deployed and interoperate.

C2 systems are unlike first come, first serve networks; they are a priority system. Rechtin (1991) described the challenge associated with many commanders directing and controlling the systems in the SoS network as follows: "With many individuals calling for priority, someone has to keep order. Someone has to command and control the C3I system."[10] However, in a system of systems, in which combatants could comprise of international partners and across different domain forces, there would be commanders holding similar level posts and conflicts could arise during operations if the reporting and operations structure of the SoS were not clear.

Having well-defined roles and responsibilities identified for the systems in the SoS network before actual deployment or operations could help to prevent potential conflicts and potential instabilities to surface during SoS operations.

3. Use of Common Ontology within System of Systems

As described in Chapter I, Section A, ontology helps to represent information so as to facilitate information sharing and reuse. With regards to multi-system interoperability, having a C2 ontology would help to present the exchanged data and relationships between these data in a consistent format, over all systems (or at least within clusters of systems which interact more often together) such that there would be less need of a translator in the interfaces between subsystems in the SoS.

Besides a common C2 ontology, efforts should also be made on the command and control semantics, such as understanding of threat characteristics

[10] C3I systems refer to command, control, communications and intelligence systems.

and their classifications, between forces to facilitate the information sharing and exchange. Having a consistent understanding and description of military terms would definitely aid communication and understanding between forces and with international partners with the same ontological understanding.

4. Systems Integration

a. System-to-System Connection/Coupling/Cohesion

Systems integration provides potential in improving in the overall performance of the system of systems. Systems are integrated to create the new capability that would not be achievable without the joining of the systems. For the interoperability of the systems to work, one would need to identify and plan for the connection, coupling, and cohesion between systems. Intersystem semantics, interaction conventions, and symbology would need to reconciled and made consistent.

The integration of systems would also result in these systems experiencing a loss. The loss can take any form, e.g., individual system capability loss, opportunity loss, energy loss or financial loss. Trade-off analysis could also be conducted between potential systems to be integrated to identify if the cluster of systems would perform better or have higher reliability in the overall system if interacting in alternative methods, e.g., being connected in hybrid star-bus network topology instead of a linear bus network topology.

The level of coupling and cohesion between systems would determine the direction, type and amount of information flow between these systems, and thus would directly affect the network traffic in the data-links between these component systems. Segmenting systems based on which systems they will only be communicating with, eliminating unnecessary data/information packages and directing data/information messages to select target system nodes instead of broadcasting the messages to all in the network of systems could help to reduce the network traffic and improve the timeliness performance of information sharing and exchange.

To integrate systems, some factors that should be taken into consideration include performance characteristics (including considerations if a system should continue to operate in a deteriorated state or switch to a fail-safe mode if significantly damaged) and possible emergent (positive or negative) properties of the SoS or sub-systems. These factors could help to form a baseline in determining the suitability of the integration and the performance to be expected of the SoS in various situations, such as loss of connection between two systems or failure of a particular system node.

b. Legacy vs. New Systems

Legacy systems are obsolete or old systems, which could have lesser processing capabilities and old technology, but they may still be useful in augmenting the military's warfighting capabilities. In planning for interoperability between legacy systems and new systems, which should already follow the network architectural ontology requirements and perhaps an open architecture integration concept, there is a need to consider the interim integration of the legacy systems to the SoS and easy detachment of these legacy systems from the SoS network. Planning for the temporary inclusion of the legacy systems and for their eventual retirement from the system of systems network would reduce complications in the transitioning phases. The actual implementation of upgrading the legacy systems to work in the SoS network and their eventual phase-out should also be done in phases, in which select legacy systems are upgraded or phased out over planned out periods.

Introduction of new systems into the SoS network should also be carried out in phases so as to cater for in-between phases testing to ensure there is no complications or negative emergence behavior resulting from the integration.

c. Integration Testing

With the large number of systems to be integrated together in a SoS, adopting a phased, incremental integration and testing approach could help

to identify and reduce network externalities and counter negative emergence. Measures could also be introduced to minimize the occurrence of network externalities or negative emergences that cannot be removed entirely.

Before testing could be carried out, there must be clear documentation of the connection, coupling and cohesion that exist between the systems and the interface messages to be exchanged between them. Test procedures, which describe the expected operations of the interfaces between systems, should be documented and used in functional testing. Following which, functional testing of smaller clusters of systems can then proceed before the number of connections between the systems in the SoS increase and testing continues.

5. System Stability

As discussed in Section A of Chapter I, stability is desired in operational military systems, especially those with the capability to deal physical damage to other systems. The example covered highlighted the fire control system, which could potentially result in fatalities if it were unstable, e.g., opening fire on targets when not commanded to.

a. Local and Global Stability

Separately, individual systems and smaller clusters of systems are preferred to be stable sub-systems or systems. Stability of a system relates to its reliability and, if stability is poor, system breakdown or failures could ensue and result in subsequent breakdown of the rest of the SoS network, depending on the connection network of the systems. Besides reliability, stability of a system also includes accuracy and precision of data transmission. If the data/information packages are not sent to and received by the correct system node in the format as expected, the overall system comprising of the interacting systems becomes an unstable system. Stability or metastability of the system should be maintained regardless of introduction or removal of a component system from the SoS.

Systems are mostly metastable within the lifespan of the system and may contain miniscule instabilities. As systems grow in size and complexity, they become increasingly easy to be affected by slight disturbances in the SoS operating environment, even if introduced by other component systems connected to the SoS. System instabilities could be a result of software deficiencies, which can only be identified through thorough testing of the interfacing software. With the SoS network spanning across heterogeneous component systems, it may be impossible to rid the SoS of all system instabilities, some of which may appear as network externalities or emergence. Nonetheless, steps should be taken to ensure that if these network issues are observed, the SoS architect should identify control measures to prevent further occurrence. Integration planning, design and implementation of the SoS should be conducted in careful and detailed processes to ensure that as the system of systems evolves, the overall system will remain at least metastable over its lifetime.

b. Operator Training

For the smooth operation of the systems in the SoS and the SoS itself, operators manning the interfaces and data-links should undergo training for the relevant system(s) or sub-system(s). Training would provide the opportunity for new operators to understand and learn about the technicalities and functionalities of the system that they are to work with. With the increased connectivity between NCW systems, the influx of data/information could overwhelm an untrained operator, and make him/her less effective in responding.

6. Information Security

Interoperability between large numbers of systems requires the backbone of a network-centric concept. Network-centric operations involves synchronized execution of distributed operations, widespread sharing of situational awareness and decision-making data. To achieve interoperability, they would require a dependable underlying information and communications infrastructure.

> The disruption or denial of computation or communications connectivity and the corruption or destruction of data would highly degrade or even render ineffective the network-centric approach to operations. The greater the dependence on information-sharing and communications capabilities, the more attractive attacks become against them—by both highly sophisticated and less sophisticated adversaries—to undermine U.S. operations.
>
> As a result, information assurance[11] (IA) provided by protecting information and communications systems against the threats of adversaries, is seen as a vital part of network-centric warfighting capabilities. (Committee on Information Assurance for Network-Centric Naval Forces, 2010)

Note that cybersecurity vulnerability and information assurance vulnerability were viewed as inseparable and were treated as such in the report.

Cybersecurity threats can be broken into four types, namely: remote access, close access, life cycle or supply chain insertion, and insiders, with the common intention of disrupting system functions, modifying data and/or stealing data. These "threats change on a timescale much shorter than the typical Department of Defense acquisition cycle for developing and deploying cybersecurity technologies." (Committee on Information Assurance for Network-Centric Naval Forces, 2010) Along with the increasing reliance on commercial information technology systems in the conduct of warfighting, the U.S. Navy faces a serious cybersecurity threat to their warfighting capability.

A technical response to cyberthreats and information assurance needs of a Naval NCW proposed in the *Information Assurance for Network-Centric Naval Forces* could be applied to other forces. Planning for IA involves risk assessment, risk mitigation and actual implementation of these risk mitigation strategies. For risks that cannot be mitigated or reduced, steps should be taken to remove these risks through changing the design of the network architecture.

[11] Information assurance is defined in the Department of Defense instruction documents as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities (Committee on Information Assurance for Network-Centric Naval Forces, 2010).

The architecture that the SoS network is built on should be designed according to a set of principles that address the essential characteristics of a system for assuring information and counter vulnerabilities resulted from poor planning for information assurance and overarching system weaknesses. The process of system architecture development should also be iterative and adaptive to ensure that the resultant SoS will remain robust in the despite emerging threats and technological changes.

An IA roadmap could also be formulated using the suggested elements compiled for an advanced naval IA research program covered in Appendix I, Table 9. These elements could be prioritized and implemented based on the needs of the SoS.

7. Concept of Operations

Concept of Operations (CONOPS) is:

> [a] verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. The concept is designed to give an overall picture of the operation. Also called commander's concept or CONOPS. (Joint Chiefs of Staff, 2010)

As such, CONOPS should be driven by the mission requirements. Concept of operations of the SoS should be correlated with the architectural design of the SoS as the mission requirements which drive the concept of operations should also drive the SoS network architecture design and operations.

> CONOPs, as described in CJCSI 3170 JCIDS series, are written to describe how a joint force commander may organize and employ forces in the near term (now through 7 years into the future) in order to solve a current or emerging military problem. These CONOPs provide the operational context needed to examine and validate current capabilities and may be used to examine new and/or proposed capabilities required to solve a current or emerging problem. (Defense Acquisition University, n.d.)

CONOPS can also represent the guidelines in which combatants should follow in their missions and thus should be clear and non-conflictive with the

mission requirements. It is the responsibility of the commander in charge of the sub-mission group to make necessary efforts to ensure the CONOPS are clear and applicable to the relevant missions and correctly propagated to the subordinate combatants.

8. Management of Change Requirements

Requirement changes are not uncommon and could require numerous changes or high-impacting changes to the SoS network architecture, CONOPS, etc. With turnovers of commanders in the military hierarchy, there would be a change of the major stakeholders of the SoS. Different individuals would have a different idea of how they would command the system or use the system to carry out their missions. Changing threat demographics, such as a higher dependence on unmanned assets versus manned systems, would also cause mission requirements to change with time.

A system to manage changes such as introduction of an approval forum to prioritize and/or control change requirements and logging down a description of changes made could help to regulate the changes made to the SoS. The SoS is comprised of multiple systems and owners for SoS configurations spanning multiple forces or even international ally forces. Any change raised could ultimately affect the rest of the other systems or could cause a reduction in the overall set of capabilities of the SoS network or of sub-clusters of systems.

VI. MODELING OF MULTI-SYSTEM AND TARGET-RICH ENVIRONMENT

A. PROBLEM

Intersystem interoperability requires connection, cohesion and coupling between these systems. When the quantity and variety of systems participating in the multi-system network increase, the ability to achieve a certain level of performance in terms of timely transmission or exchange of data/information could influence the result of a joint SoS mission.

B. BACKGROUND

With increasing deployment of unmanned platforms (for both own-force and adversaries) and increasing intersystem linkages in today's battlespaces, it is pertinent for decision-makers to consider the tradeoffs between timeliness of data/information exchange, amount of data/information that is sent/exchanged and the number of system nodes within the overall network of systems or system of systems. Integration of multiple, heterogeneous systems can increase mission effectiveness in combat but could also result in delays and security weaknesses in the overall system if ill-planned or ill-designed.

The mission effectiveness of a SoS, in dealing with fast-paced and rapidly changing battlespaces, is highly dependent on the efficiency and effectiveness of acquiring situational awareness of the SoS operational environment and the command and control of the SoS in carrying out sub-missions to accomplish the overall mission. To be able to keep up with the fast pace of network-centric operations, the information dissemination, in-system processing and relaying of the information for other sub-systems to take action on would need to be timely.

C. APPROACH AND ASSUMPTIONS

Time delays within the SoS network would result in component systems receiving key data or information late. Actions could be taken on targets late or

not be acted on at all, as the target could have moved out of the system's weapon range. Own-force systems or platforms could be destroyed by the adversary in the process. This, in turn, could result in the mission failure of the SoS.

A pilot study was conducted to assess the time delays resulting from varying the number of messages being sent from an individual system node to the rest of the nodes in the SoS network and the number of system nodes layers which exist between the end nodes and the originating system node. This will provide insight into the impact of adding nodes to the overall system or increasing the message traffic to the duration of message propagation to the end-nodes of the system. For this study, a network model was designed and developed to represent a generic message transmission/broadcast network architecture, in which multiple systems are interconnected and message packages are sent from the originating system to adjacent systems and these systems subsequently propagate the information to their adjacent systems.

The initial network model comprised a single channel for the transmission of data/information from the message generating system node to the end nodes of the SoS. Thus, it is referred to as the Single-Channel Data Transmission Simulation Model. This network model was then modified to accommodate a dual-channel data transmission configuration (referred to as the Single-Channel Data Transmission Simulation Model) to study potential improvements of the overall SoS performance in terms of data/information propagation timeliness. These network models and the interactions between the systems in the architecture are described in detail in Section F.

Key assumptions used in the design and development of the model include the following:

- Processing delay at individual system nodes is simulated as an exponential distribution[12] with a mean time of 1 simulation time unit. Slight delays are introduced to represent the time required to parse, re-format and present the information received in the display by the subsystem. Information was propagated further to other nodes downstream, with a mean simulation time unit of 1.
- The maximum number of messages that can be processed by each system node is 3, simulating 3 message packages, carrying data/information as the maximum number of messages that can be managed by an individual system node.
- Connection, coupling and cohesion are represented in the model through use of physical data-link connections between the system nodes, presence of processing delays at data/information receiving nodes and feedback of received data/information respectively. It is assumed that the information sent from a system node is received correctly, i.e., the data/information content sent by the sender node is received as the same content when received by the receiver node.
- There is no restriction on the size of the data/information packages sent to or received by the system nodes and there is no restriction on the number of packages queued to be processed by individual system nodes.
- Each system node is connected to one upstream parent node and could be connected to one or to two downstream children nodes.

D. SOFTWARE USED

ExtendSim Suite 8.0.1 was used to model a multi-system and multi-target environment and assess the problem of interoperability by investigating the connection, coupling and cohesion factors across these interconnected system nodes.

The model developed in ExtendSim used discrete event modeling components to replicate message transmission between processing system nodes. The use of ExtendSim allowed for the logical representation of an

[12] Exponential distribution is used to randomize the waiting time to process different data/information packages as these packages could require different times to parse and decipher. Exponential distribution is the only continuous memoryless random distribution, making it more suitable as the process times of individual data packages are non-dependent on previously processed packages (Weisstein, 2012).

integrated system and the visual appreciation of message propagation amongst these nodes through 2D animation, which also facilitated troubleshooting. Specifically for this thesis, ExtendSim allowed for the ease of modeling dynamic interaction and processing delay of messages arriving from different channels and the extraction of overall SoS performance variables based on the capacity of data/information handling at individual nodes. In addition, the data output was extracted to Microsoft Excel for further analysis of results.

E. HARDWARE USED

The platform used to run the ExtendSim model was an Intel® Core ™ i5 CPI[13] Dual Core Dell laptop with 4GB of RAM (read-access memory), running on a 64-bit operating system and Windows 7. Note that the memory limitations of the laptop only allows for a maximum of 76 system nodes to be modeled in the ExtendSim software environment.

F. MODEL DESCRIPTION

1. Single-Channel Data Transmission Network Model

To simulate a network of system nodes in ExtendSim, the "Local Area Network" discrete event modeling example available in ExtendSim Suite 8.0.1 was referenced. Using a similar concept of information exchange between nodes in a network and representation of information as physical items in the system as the LAN model, system nodes were developed as individual hierarchical blocks[14] comprising of *Queue* and *Activity* blocks to imitate network buffers and system processors respectively. Other ExtendSim components such as *Get*, *Equation*, *Select Item In* and *Select Item Out* blocks were used to read, update and extract relevant performance characteristics of the SoS network architecture. *Create*

[13] CPI is clock cycles (alternating current pulses) per computer instruction that is being performed by the computer processor (Rouse, 2005).

[14] ExtendSim's hierarchical capability allows for basic modeling constructs (such as a group of connected blocks) to be combined into a single, higher level construct, called a hierarchical block. Hierarchical blocks is a special block that usually has a group of blocks nested within. Here, these blocks are used to help organize the model logically and enhance comprehension (Imagine That Inc., 2010).

blocks were used to generate data/information packages in the main message generating system node and other system nodes to generate and replicate messages correspondingly to be propagated to adjacent downstream system node(s). To track the elapsed time for data/information packages to arrive at the end system nodes and to return back to the originating message generating, item attributes such as message number (MsgID) and item or data/information generation time (BirthTime) were used. To ensure that each message had completed its propagation through its route through downstream system nodes until end nodes (i.e., system nodes with no adjacent nodes connected to them downstream) and back to the originating message generating system node, a counter (num_nodes) was used.

Hierarchical blocks (H-blocks) were used to group the ExtendSim component blocks to represent them as individual system nodes. A generic system node H-block representing a generic system node and its corresponding component block breakdown are shown in Figure 10. Enlarged sections of the generic system node are provided in Figure 11. and Figure 12. for easier reference. Each generic system node has two input and two output connectors with upstream or downstream connections as described in Table 1.

Connection	Description
(blank) input connection	Allows system node to be connected upstream to its parent node to receive data/information from it.
Fdbk input connection	Allows system node to connect to child/children node(s) to send feedback.
Out output connection	Allows system node to connect to up two downstream to two children system nodes to send data/information to them.
Return output connection	Allows system node to be connected downstream to up to two children system nodes to receive feedback from them.

Table 1. System Node H-Block Connection Representations

The message generating system node is represented as a black-colored system node H-block (Figure 13.) to differentiate it from the generic system nodes. Enlarged sections of the generic system node are provided in Figure 14. and Figure 15. for easier reference. Although the components of the message generating system node are mostly similar to the generic system node H-block, it contains a *Create* block, which generates data/information packages for propagation to the other downstream system nodes in the SoS. The components also contain an Exit block to remove the items from the simulation at the end of their lifespan at the originating message generating node. Each item is considered to have reached the end of its lifespan when it is completed a cycle of propagating from the message generating node to an end-node and back to the message generating node.

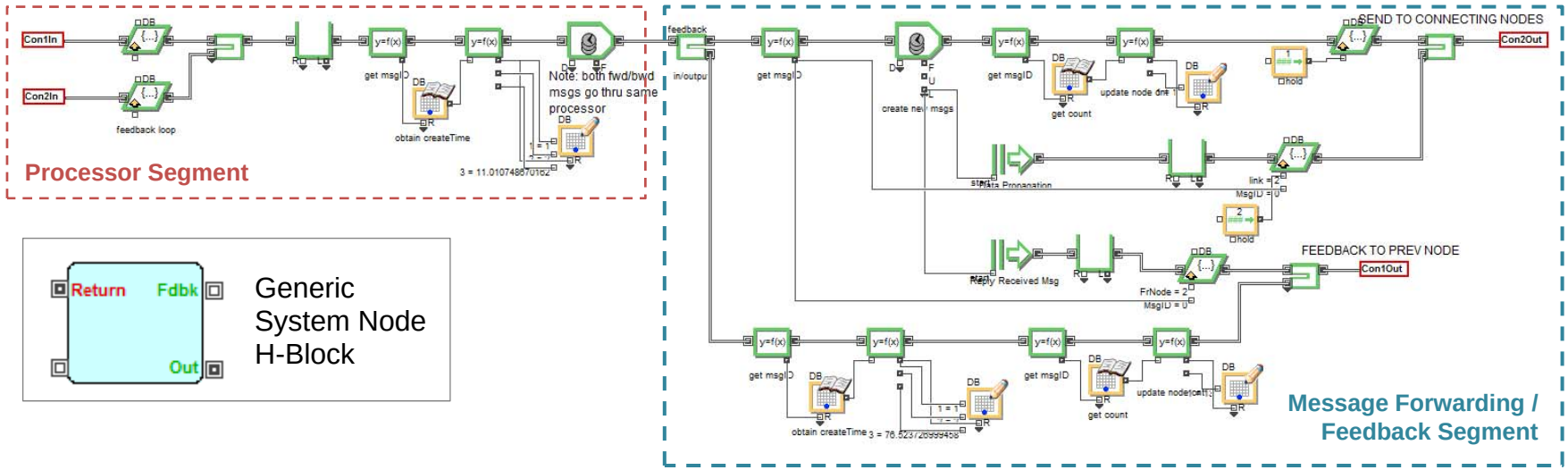

Figure 10. Generic System Node H-Block and Sub-Components

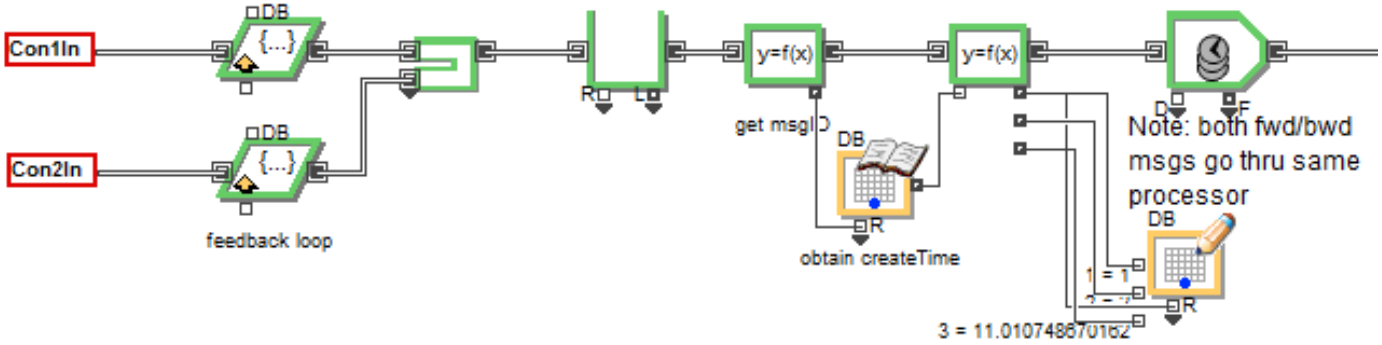

Figure 11. Generic System Node Processor Segment

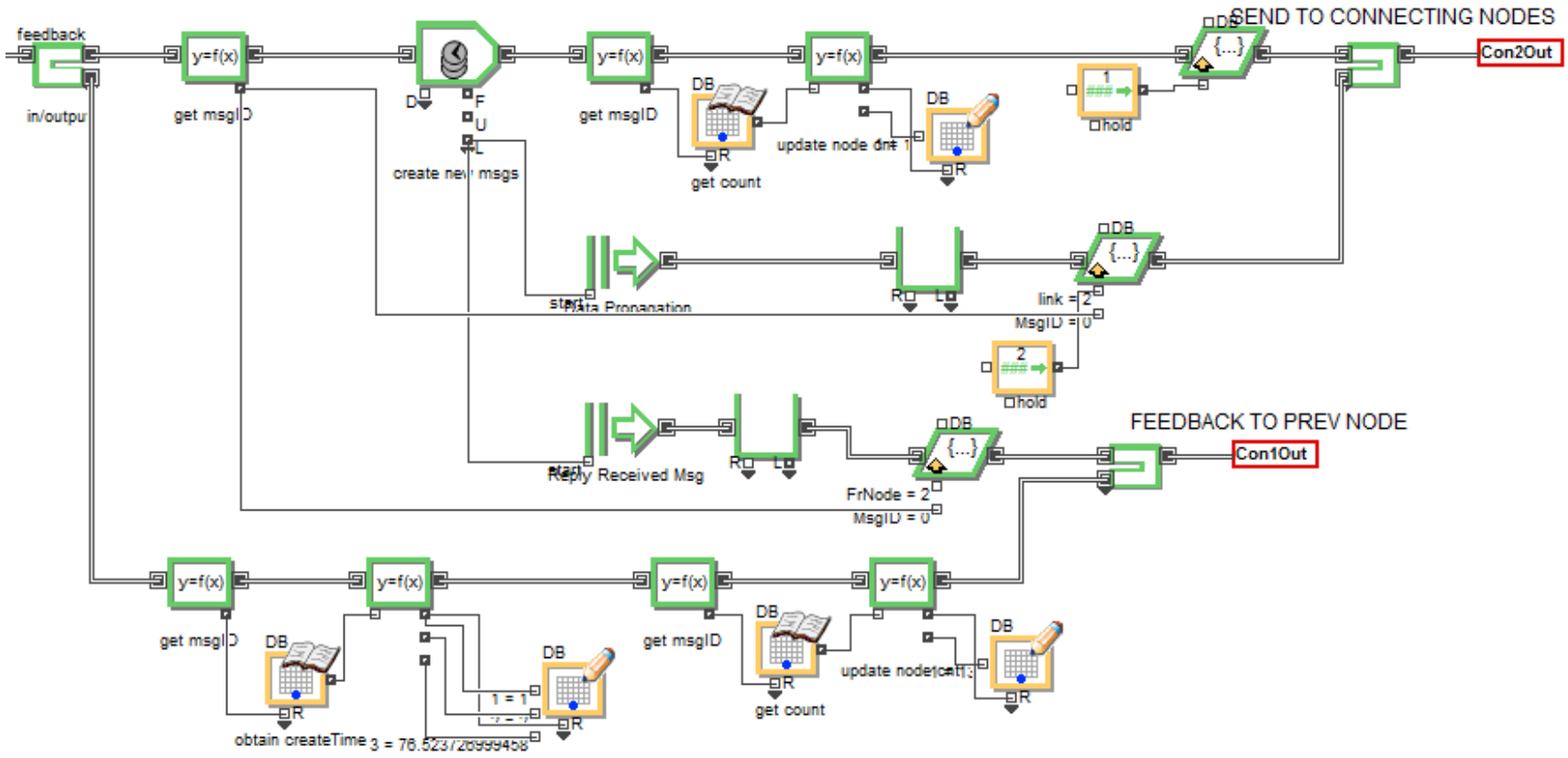

Figure 12. Generic System Node Message Forwarding/Feedback Segment

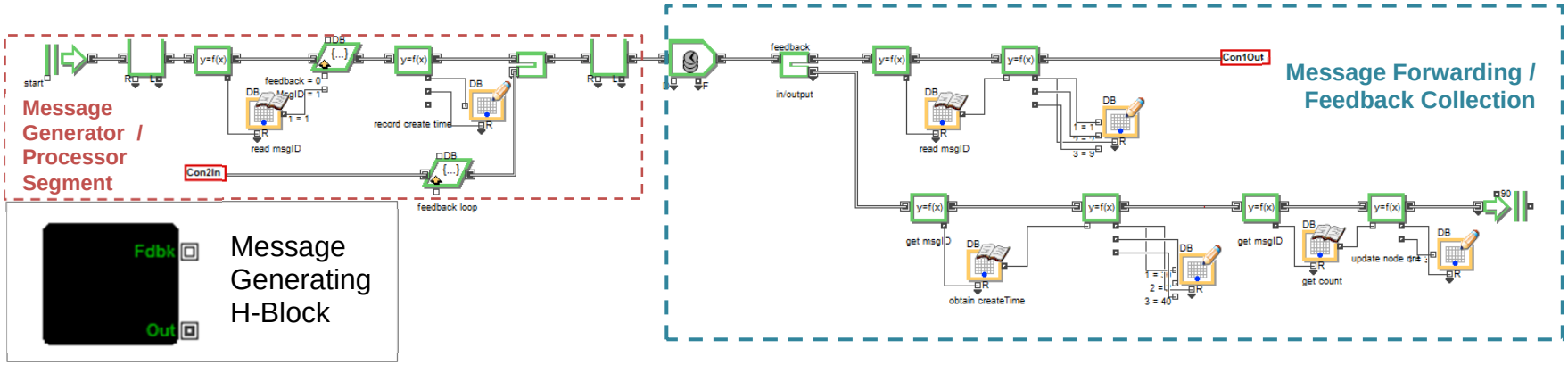

Figure 13. Message Generating H-Block and Sub-Components

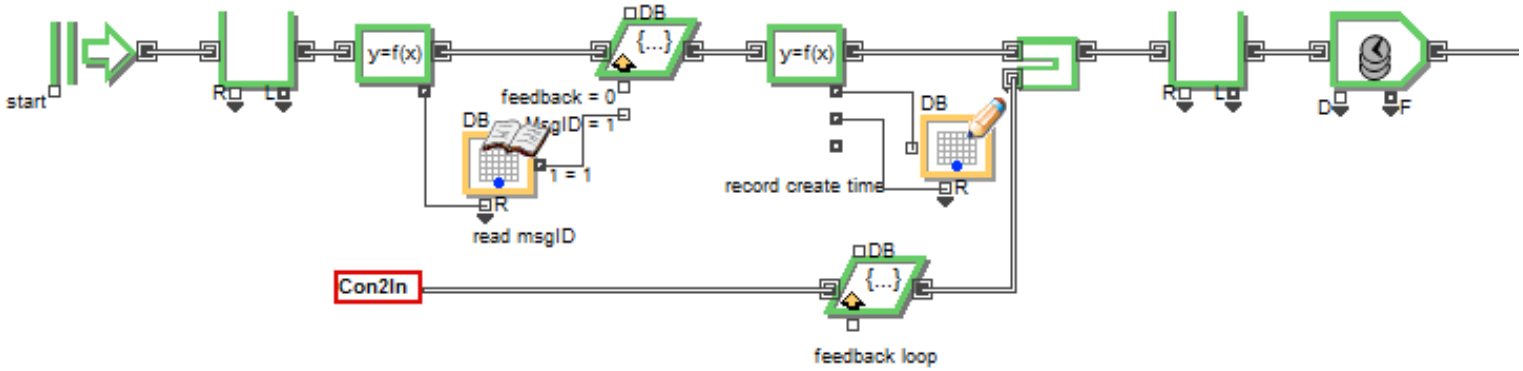

Figure 14. Message Generator / Processor Segment of Message Generating System Node

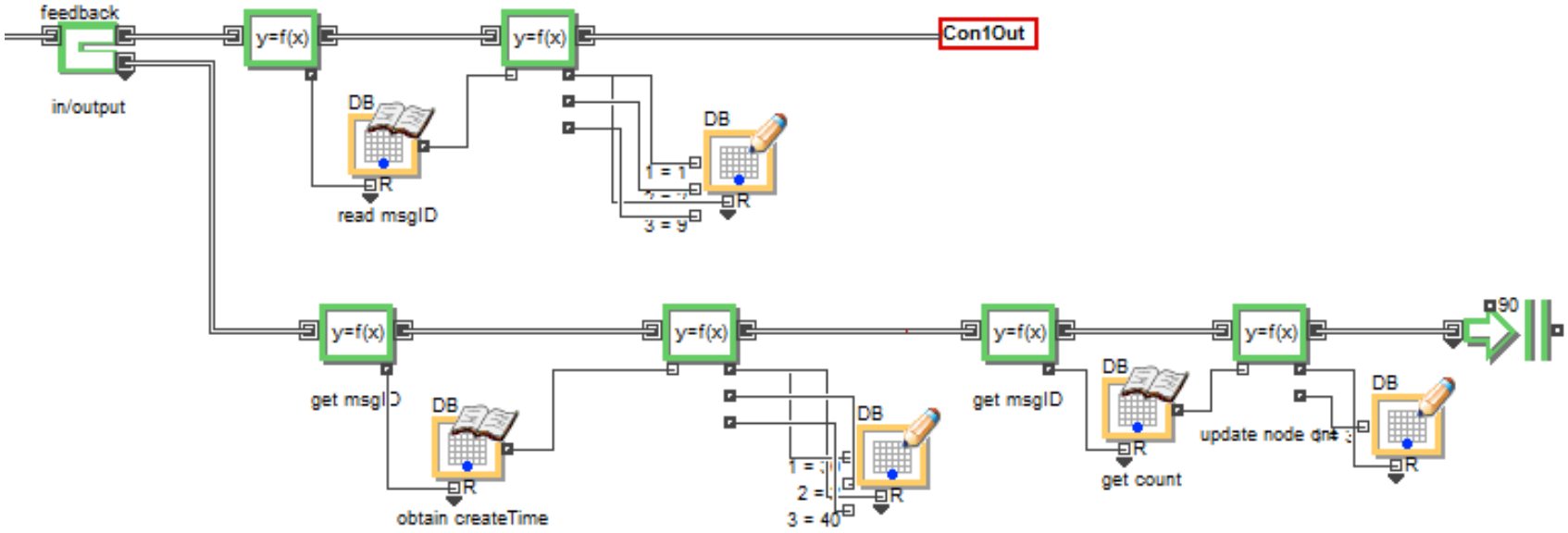

Figure 15. Message Forwarding / Feedback Collection Segment of Message Generating System Node

These H-block system nodes (both generic and message generating system nodes) form a network architecture of inter-linked system of systems. Through extending new child generic system nodes along the end-nodes of the SoS, the simulation was expanded to assess performance changes of the data/information propagation to all systems in the SoS and vice versa. Simulation runs comprised of varying number of system nodes in the SoS configuration were conducted with 3 generic system nodes as the simulation basic model. Subsequent runs were conducted starting with a SoS comprising of 5 generic system nodes, until there were 75 generic system nodes in the SoS. System node additions were doubled by the number of nodes of the previous layer of system nodes. The overall SoS network architecture of 7 nodes and 75 nodes are depicted in Figure 16. and Figure 17. , respectively. Refer to Appendix II for network architecture illustrations of various number of system node layers. Table 2. illustrates how the number of layers of system nodes corresponded with the total number of generic system nodes in the SoS network modeled.

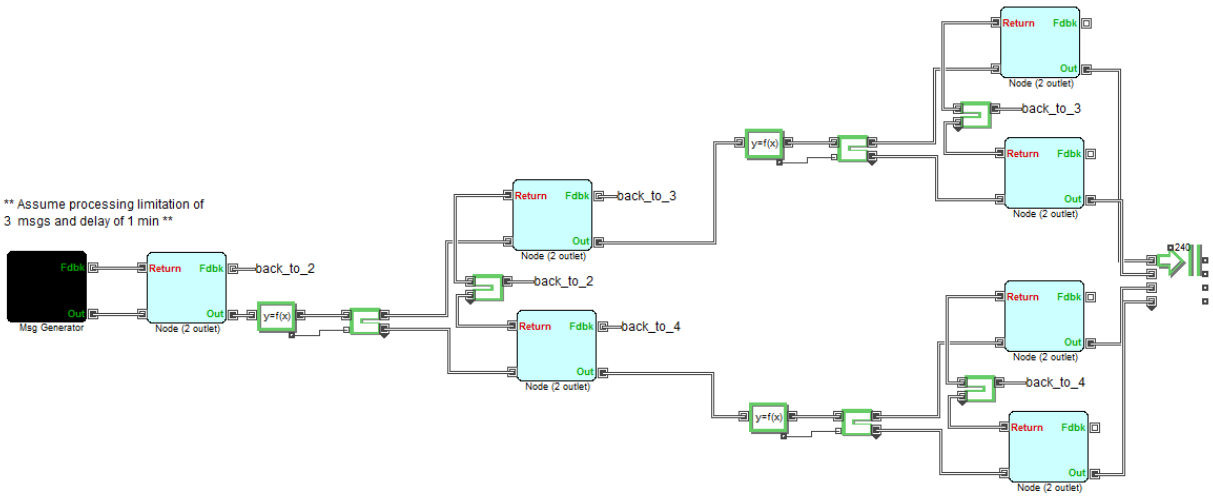

Figure 16. SoS Network Architecture of 7 System Nodes

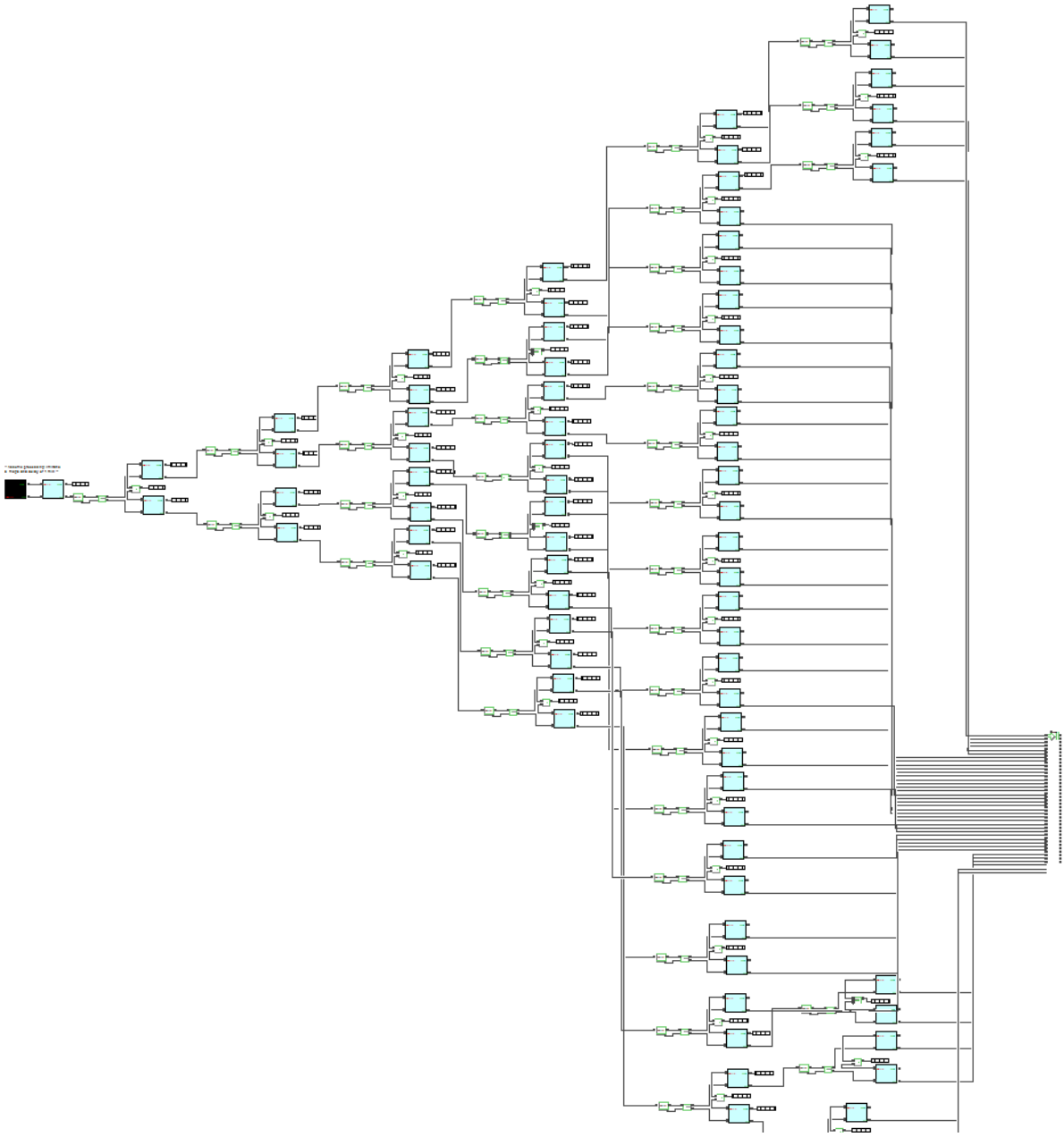

Figure 17. SoS Network Architecture of 75 System Nodes

Number of Layers	Number of Generic System Nodes
1	1 node (single node connected to message generating node)
2	3 nodes (an addition of double the number of nodes in the 1st layer are connected to the outputs of the single node in the 1st layer)
3	7 nodes (an addition of double the number of nodes in the 2nd layer are connected to the outputs of the 2 nodes in the 2nd layer)
4	15 nodes
5	31 nodes
6	63 nodes
6.5	75 nodes[15]

Table 2. Number of System Nodes Corresponding to Number of Layers in SoS Network

In addition to varying the number of nodes in the system, the number of messages (or items) being created at the message generating system node at the start of every run was varied to simulate a multi-system and multi-target operating environment. As the number of systems in SoS network increase, more hops are required for the data/information packages to reach the end nodes and back to the originating system node, resulting in an increase in the time elapsed for the data/information packages to arrive at the end nodes and reach back at the message generating node. In addition, having a different number of systems in the SoS and a different amount of targets needed to be detected, processed, identified, and action-taken-against would vary the amount of information being sent from a single node to all other nodes in its network. Interoperability means interacting systems would need to update other systems of its own statuses and vice versa, e.g., if one system is operational or incapable of operations, send command and control instructions and exchange situational picture of their environments. As the number of targets in the SoS environment increase, the

[15] Note: Due to memory limitation of the laptop used to run the simulation, only 12 nodes could be added to the sixth layer of the SoS network.

number of these data/informational packages would naturally increase. This change in targets is modeled in ExtendSim through increasing the number of messages sent by the message generating node.

Three databases (Send, Receive and Feedback) were defined in ExtendSim to store message information (MsgID and message BirthTime), and to record time elapsed (from message creation time) for messages to reach all end system nodes and maximum time elapsed (from message creation time) for message feedback to arrive back at the message generating system node respectively. Through the use of *Equation* blocks, these elapsed times were updated at various system nodes as the message (or item in ExtendSim's context) passes through the Activity blocks in individual system nodes. The resulting output databases (Receive and Feedback) are then extracted and processed in Excel to obtain the interoperability performance results of this network architecture.

2. Dual-Channel Data Transmission Network Model

The single-channel data transmission network architecture utilizes a single data-link in which both types of data/information packages, regardless of message propagation or acknowledging receipt of the message is done through the same data-link channel. This data-link transmission configuration will affect the efficiency of the system nodes in the middle of the network hierarchy as these message packages will have to pass through the same processing unit of the system node. Coupled with an increasing number of targets in the environment, increasing intersystem connectivity would increase the number of data/information packages being exchanged between these system nodes. Given that the processing time of data/information packages at individual nodes is modeled using exponential distribution, the elapsed time for data/information propagation would increase with a steeper exponential increment as the number of system node layers increases. As expected, this trend increase in the elapsed

time due to an increase in the number of system node layers was observed in the simulations carried out for the single-channel data transmission network model (Chapter VII, Section C).

The increase in the number of messages broadcasted to other systems in the SoS configuration, however, was expected to result in a near linear increase in the time elapsed for data/information packages to arrive at the end nodes as feedback returns along the same data channel would inevitably cause an additional delay. This was also observed in the simulation results, as plotted in Figure 20. As the number of system node layers increases, the rate of increase in the data/information propagation elapsed time to reach the end nodes would also increase.

In an effort to improve the timeliness of key data/information packages reaching all system nodes, a secondary channel was proposed to be added to the single-channel model to direct all feedback traffic along a separate communications channel. This thesis proposed and recommended the introduction of a satellite communications link, which would allow all generic system nodes to direct immediate responses back to the system node initiating the data/information propagation, with less geographical constraints as the satellite would be within line-of-sight (LOS) of a larger area of systems. This additional communications channel is modeled in ExtendSim through redirecting all feedback outputs (from the **Return** connector) of the system nodes to a *Select Item In* collector block, which links directly back to the feedback input connector (**Fdbk**) of the message generating system node. No modifications were made to the components within individual system nodes and the data used/extracted from the previously defined ExtendSim databases. The resultant network model for a 7-node SoS network architecture model is shown in Figure 18.

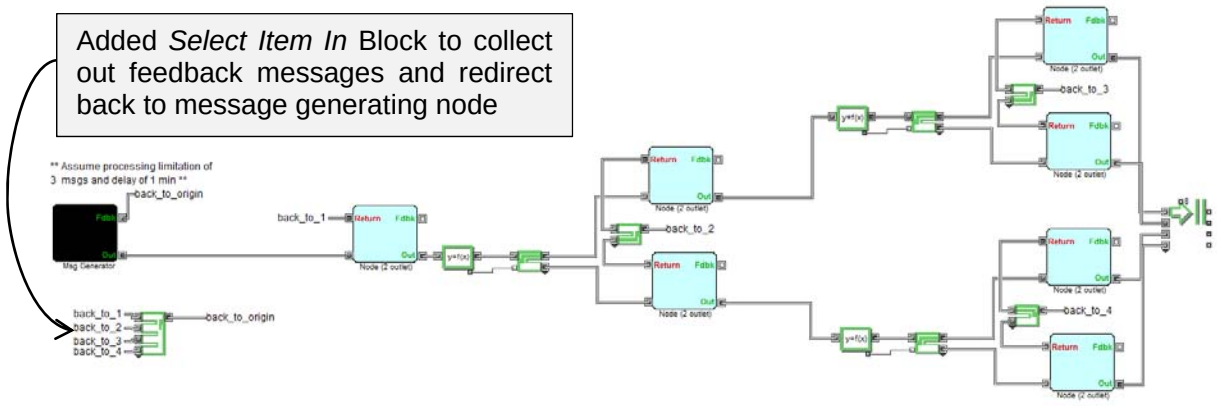

Figure 18. Modified SoS Network Architecture of 7-Node System

The results obtained from the simulation runs of these network architecture models will be tabulated and discussed in Chapter VII.

VII. DISCUSSION OF RESULTS

A. PERFORMANCE METRICS

As described in Chapter VI, the ExtendSim model was designed and developed to assess the impact of increasing the number of systems participating in the SoS interoperability network and increasing the network traffic between these systems on the efficiency of message propagation in the SoS. Increased network traffic would be observed in a SoS due to both increasing system participation and increasing presence of targets in the SoS operating environment. Thus, to quantify the performance of the multi-system network model, the following performance metrics are used:

Performance Metric	Description
Mean elapsed time to arrive at end-nodes	Average time taken for data/information package to finish propagating to all nodes (which ends with the end-nodes).
Maximum elapsed time to arrive at end-nodes	Maximum time taken for data/information package to finish propagating to all nodes.
Mean elapsed time to return to message generating node	Average time taken for data/information package to propagate to all nodes and acknowledgement messages are sent back to the message generating node from all individual system nodes. (Note that every system node was designed to return an acknowledgement of message received automatically to its parent node.)
Maximum elapsed time to return to message generating node	Maximum time taken for data/information package to propagate to all nodes and acknowledgement messages are sent back to the message generating node from all individual system nodes.

Table 3. Performance Metrics Description

The performance metric, “elapsed time to arrive at end-nodes,” provides a measure of how timely the data/information is broadcast and received by the nodes within the SoS. Shorter elapsed times for the data/information to reach the nodes in the network would help to save time for the response actions to this data/information to be taken. The longer a data/information package takes to arrive at the node that is required to take action on, the less accurate the data/information. The environment or circumstance of the battlefield could have changed significantly during the time elapsed for message propagation to render the information useless, especially in the modern day warfare, in which technological advancements have increased the speeds of warfare systems, making timeliness data/information very important.

“Elapsed time to return to message generating node,” provides a measure of how long the system node initiating the data/information transmission would need to wait before sending subsequent information such as updates, commands or orders to the nodes. For interoperability to exist, a two-way form of communication is required to ensure that: firstly, the receiving node receives the data/information package; secondly, it acknowledges receipt of the package to the data-originating node and thirdly, the data-originating node is aware that the target node(s) has received the necessary information. In addition, this would provide a form of confirmation to the data-originating node that the target node is the correct recipient node and that the information was received accurately.

B. CONDUCT OF EXPERIMENTS

The two input variables for the simulation model runs are as follows:

- The number of layers of system nodes in the network or number of nodes in the system. (Note: This is a better measure of the system node loading on the system than the actual number of system nodes, as this variable would directly influence the duration required to traverse adjacent system nodes.)
- The number of messages broadcasted (sent) to the SoS.

For each SoS network architecture studied in this thesis, ten simulation runs were conducted for each combination set of these input variables to form the data samples obtained through these simulation runs. The output data is then tabulated in Microsoft Excel; the output data corresponds to the value of the performance metrics of the SoS.

C. USE OF SINGLE CHANNEL FOR DATA TRANSMISSION

The average time taken for varying quantities of data/information package to be delivered to the end nodes in a SoS network architecture of varying number of system nodes is tabulated in Table 4. Note that there is no specific time unit used as the parameters used in this model could be modified to suit various time units depending on the use and scale of the network model.

#Msgs / Layers	3	5	10	15	20	25	30	Remark(s)
2	0.862	1.046	2.576	3.256	3.957	5.419	6.653	3 nodes
3	2.914	4.302	6.305	8.631	11.885	13.812	16.502	7 nodes
4	5.681	6.264	9.431	14.091	18.281	21.353	25.408	15 nodes
5	7.512	8.399	13.718	19.080	25.308	32.571	36.808	31 nodes
6	9.437	11.441	19.550	29.576	37.591	46.453	54.703	63 nodes

Table 4. Average Elapsed Time to Arrive at End-Nodes

For appreciation of how the time taken by the data/information package to traverse all the system nodes to the end-nodes is distributed with changes in number of messages generated and the number of system node layers, a three-dimensional plot of the distribution is generated from the simulation run whose results are shown in Figure 19. The SoS traverse time is plotted against the number of messages for varying number of system node layers in the SoS in Figure 20. It is also plotted against the number of system node layers in the SoS for varying quantities of data packages created at the message generating node in Figure 21. It can be observed that the time taken for the data/information

package to traverse the SoS is influenced more by the number of layers of system nodes than it is by the quantity of messages.

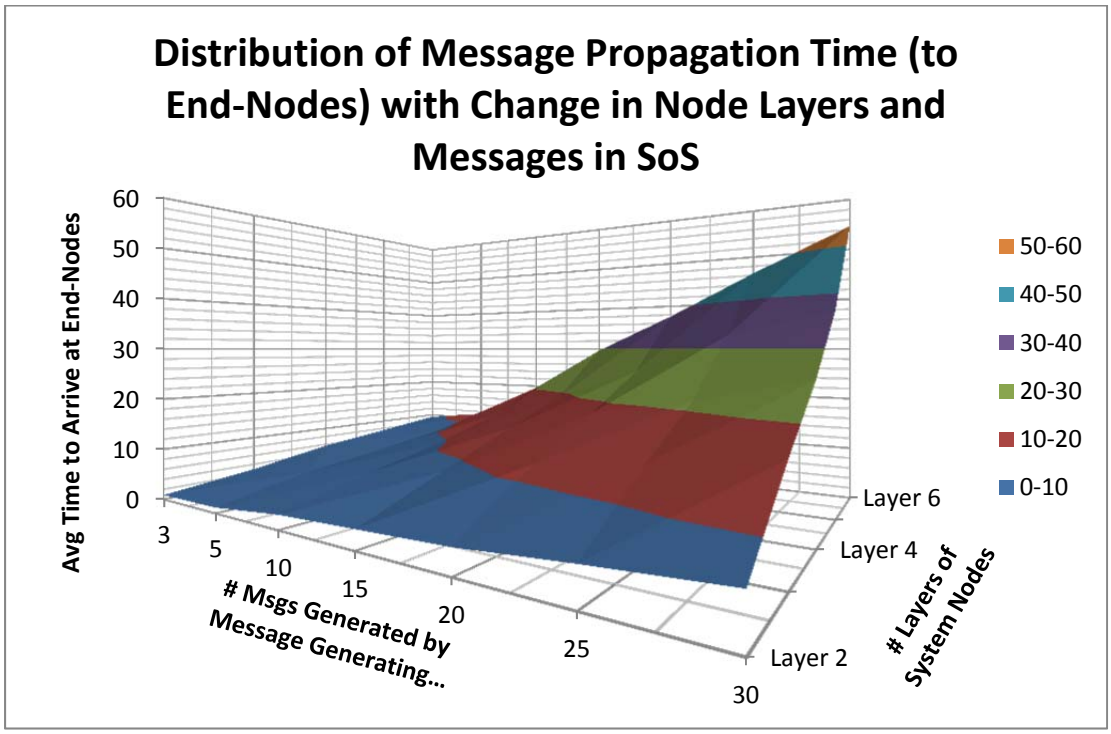

Figure 19. Distribution of Message Propagation Time in Single Channel SoS Network Model

It can be observed that the increase in the number of messages generated result in a resultant SoS traverse time that trends towards a linear profile for the network models with varying layers of system nodes (Figure 20.). As the number of system node layers increase, the rate of increase of the traverse time becomes higher. On the other hand, due to exponentially distributed processing delays incurred in individual system nodes, the SoS traverse time of the data/information packages will increase exponentially as the number of system node layers increases (Figure 21.). Similarly, as the number of messages being propagated in the SoS increases, the rate of exponential increase of the traverse time increases. Coupled, these phenomena would cause a steeper increase rate of the time taken by the packages to traverse through all

the system nodes in the SoS, causing the data/information to reach at a delayed time since the point of first propagation within the SoS.

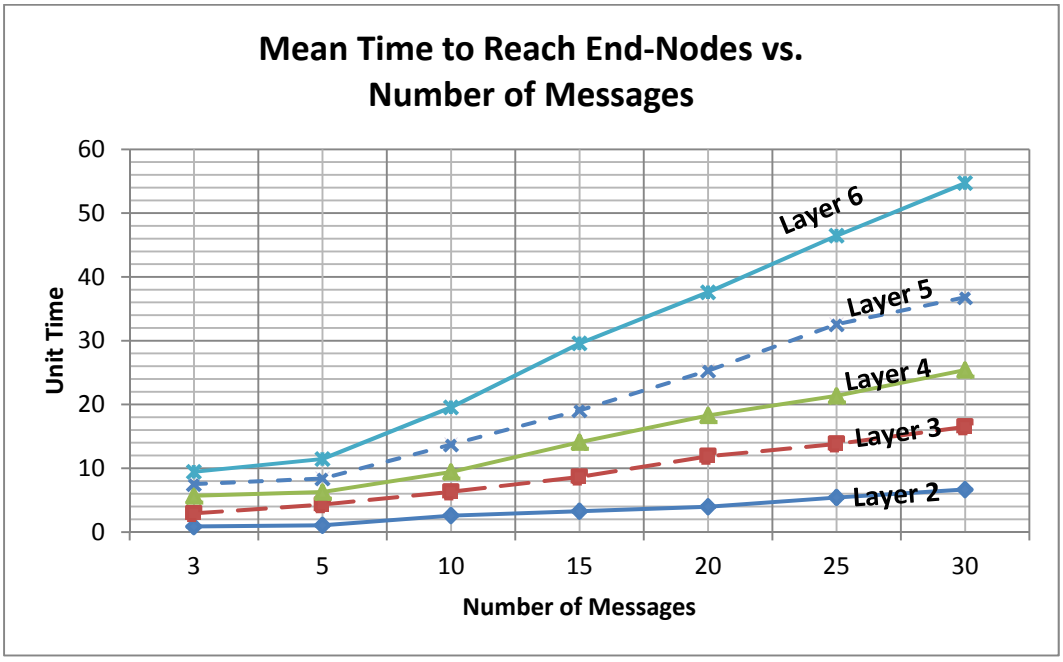

Figure 20. Trend Breakdown of Mean Time for Data-Packages to Reach End-Nodes for Varying Number of Layers of System Nodes

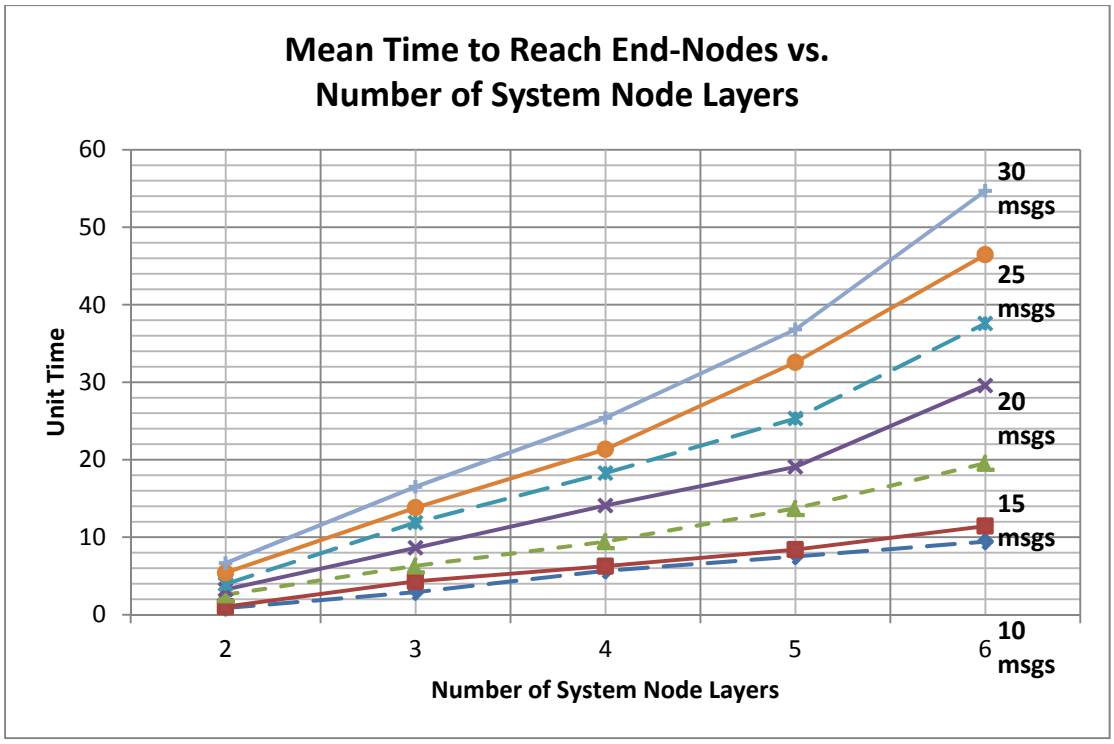

Figure 21. Trend Breakdown of Mean Time for Data-Packages to Reach End-Nodes for Varying Number of Messages

To understand the extent of the delay severity of the traverse time of the data packages, its maximum statistics for the varying number of node layers and messages sent were extracted as shown in Table 5. The tabulated data was also represented as a three-dimensional plot (Figure 22.) to show the overall trend of the traverse time delay.

#Msgs / #Layers	3	5	10	15	20	25	30	Remark(s)
2	2.924	3.064	8.641	7.604	10.123	12.933	16.391	3 nodes
3	6.008	10.350	13.365	18.392	29.771	33.249	36.004	7 nodes
4	14.039	12.314	24.820	32.004	39.979	51.960	52.902	15 nodes
5	16.285	16.323	28.852	44.505	51.564	84.178	78.647	31 nodes
6	14.890	20.088	43.298	64.422	85.441	106.706	121.390	63 nodes

Table 5. Maximum Elapsed Time to Arrive at End-Nodes

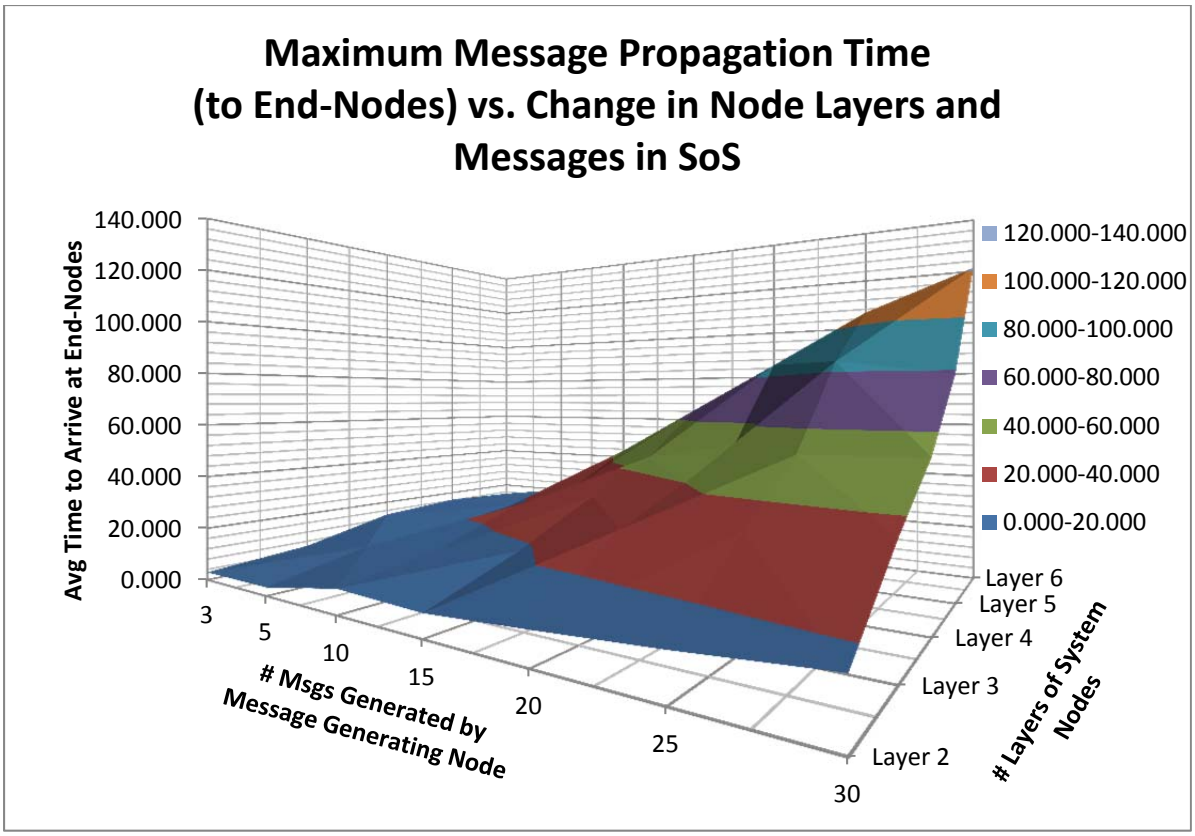

Figure 22. Trend of Message Propagation Time vs. Number of Node Layers and Messages in SoS

The maximum delay experienced by the end-nodes in receiving the data/information sent from the message generating system node can be more than twice the average delay time experienced by these same nodes. Thus, in deciding how many system nodes and amount of data/information being exchanged between these nodes in the SoS, these delay factors should be considered.

For the same set of simulation runs, the “elapsed time to return to message generating node” of the sent data/information packages were also extracted as shown in Table 6. This data was also plotted in both three and two-dimensional graphs (Figure 23. Figure 24. and Figure 25. to better assess the time delays experienced in the system.

#Msgs / Layers	3	5	10	15	20	25	30	Remark(s)
2	3.631	4.543	8.839	12.047	15.402	19.349	23.578	3 nodes
3	9.637	13.878	22.486	31.275	40.298	47.838	56.603	7 nodes
4	17.351	26.696	45.469	62.029	78.765	93.298	110.829	15 nodes
5	35.613	51.474	92.551	122.284	154.735	184.355	214.726	31 nodes
6	68.274	108.799	175.484	239.272	306.245	358.358	423.101	63 nodes

Table 6. Average Elapsed Time to Propagate to End-Nodes and Return to Message Generating Node

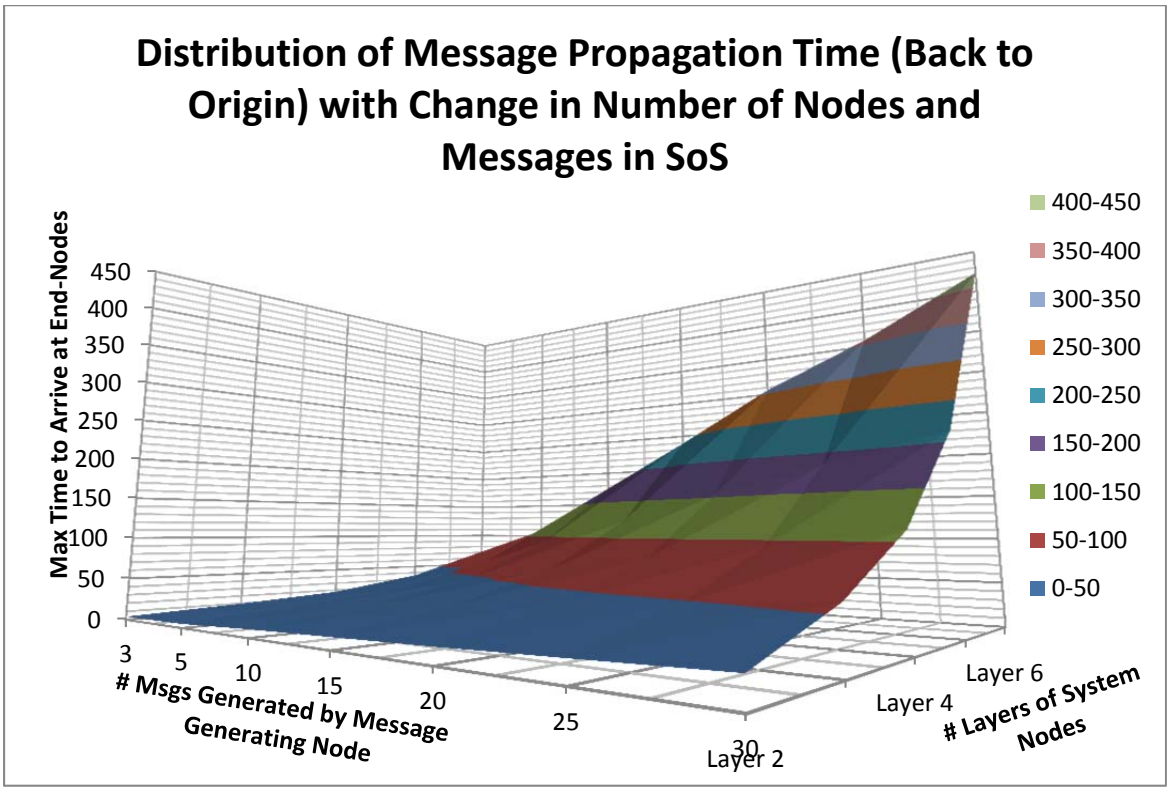

Figure 23. Distribution of Message Propagation Time for Data-Package to Return to Origin in Single Channel SoS Network Model

The mean time taken by the data/information packages to arrive back at the message generating system node (also referred to as Origin) from system nodes in the SoS differs by a wider margin over different numbers of system node layers in the SoS (Figure 24.), as compared to the SoS traverse time for the packages to reach end-nodes.

The rate of increase of delay time from birth time of the data/information package until the package is propagated back to the message generating system node is found to be steeper (Figure 25.), as compared to the incremental trend of the SoS traverse time to reach the end-nodes. This observation is caused by the exponentially-distributed delays that these data/information packages will have to undergo when they re-track the system node pathways to send acknowledgement feedback to the originating node.

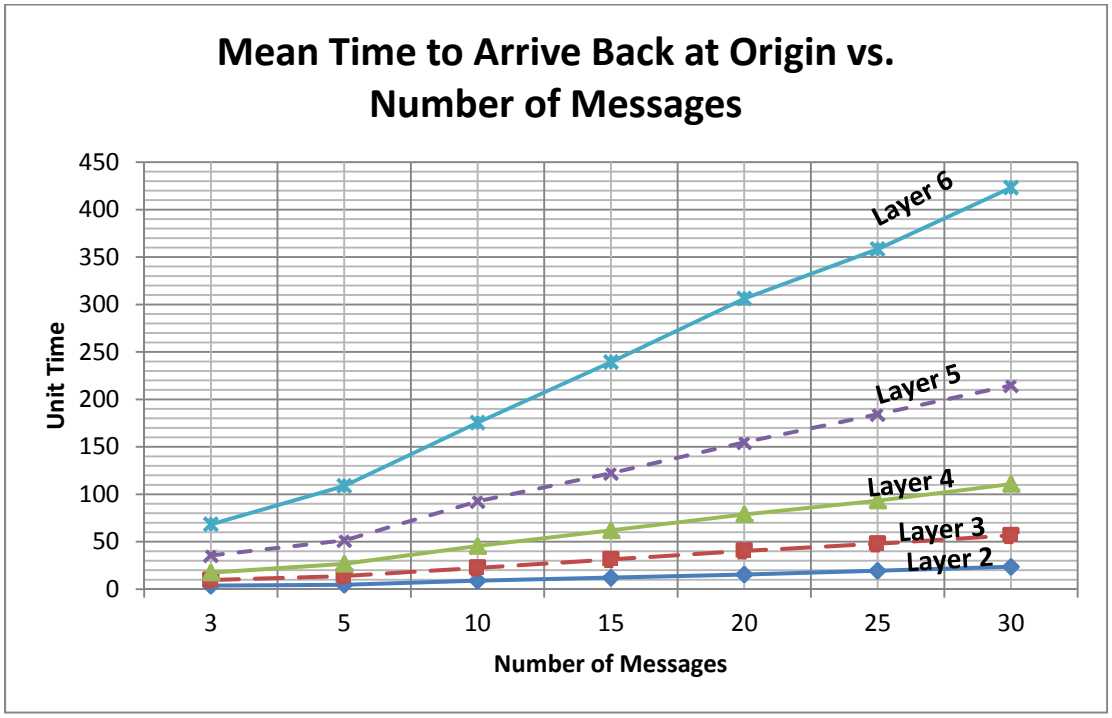

Figure 24. Trend Breakdown of Mean Time for Data-Packages to Arrive Back at Origin for Varying Number of Layers of Nodes

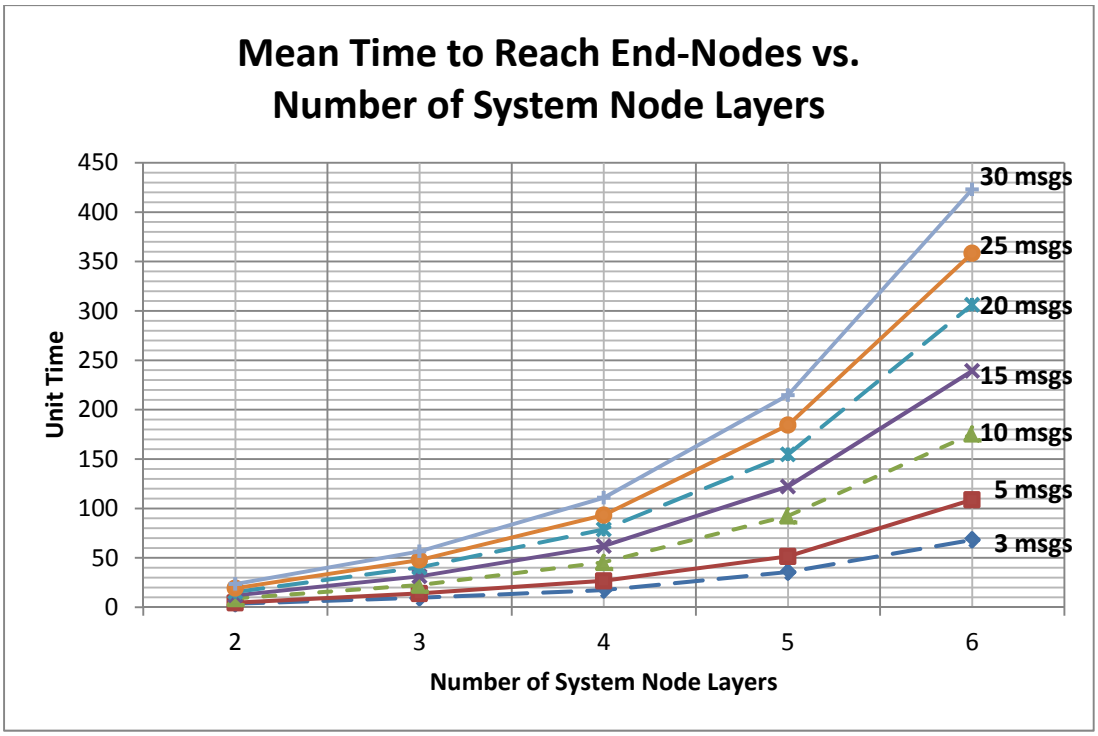

Figure 25. Trend Breakdown of Mean Time for Data-Packages to Arrive Back at Origin for Varying Number of Messages

Thus, from the simulation runs of the single-channel data transmission network model, it can be inferred that increasing the introduction of system nodes into a SoS would incur a greater cost on the efficiency and effectiveness of SoS performance than increasing message traffic in a SoS. Network architectures should be designed such that fewer delays are experienced between interacting systems, especially when the exchanges between these systems are frequent and with large amounts of data/information in the exchange. Efficiency and effectiveness of the mission conducted through NCW can then be further improved through control of the message broadcast, transmission or exchange within the SoS.

D. USE OF DUAL CHANNELS FOR DATA TRANSMISSION

The results for the simulation runs of the modified SoS network model, which includes a separate satellite communications channel for

acknowledgement messages to be returned to the message generating node directly, were obtained similarly as those extracted in Section C.

#Msgs / #Layers	3	5	10	15	20	25	30	Remark(s)
2	2.029	2.537	3.409	4.592	5.520	6.580	7.607	3 nodes
3	3.503	3.841	5.050	6.541	7.657	8.877	10.312	7 nodes
4	5.265	5.386	7.069	8.442	9.394	10.805	12.087	15 nodes
5	6.808	7.655	9.132	10.565	11.968	13.367	14.883	31 nodes
6	9.786	9.665	11.190	12.585	14.532	15.164	16.912	63 nodes

Table 7. Average Elapsed Time to Arrive at End-Nodes for Satellite Model

With the introduction of the secondary satellite communications channel into the simulated SoS network model, the time elapsed for the data/information packages to arrive at end-nodes increases approximately linearly with increases in the number of messages being propagated in the SoS and the number of system node layers (Figure 26. Figure 27. and Figure 28.). The average times required for the data/information to reach the end-nodes have been significantly reduced (Table 4. and Table 7.). The redirection of the feedback traffic from the single-channel data transmission network model has helped to reduce the delays in the data/information propagation from creation to the end-nodes. This presents added time-window opportunities for the receiving system nodes to react on the data/information.

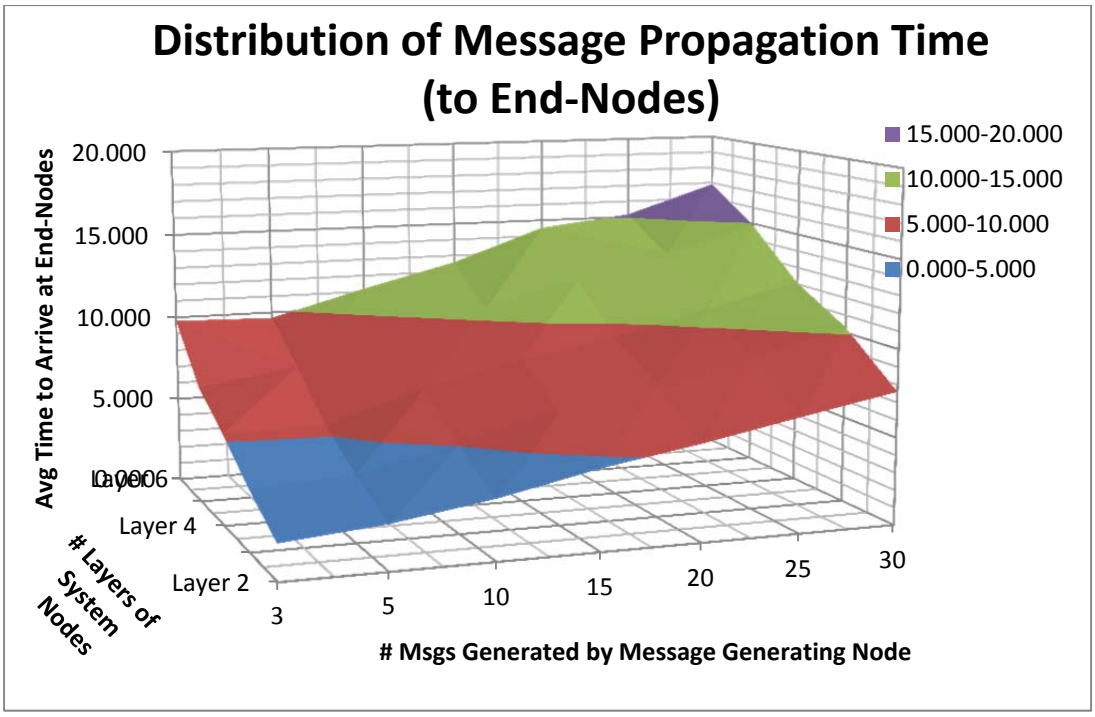

Figure 26. Distribution of Message Propagation Time in Single Channel SoS Network Model (Satellite Model)

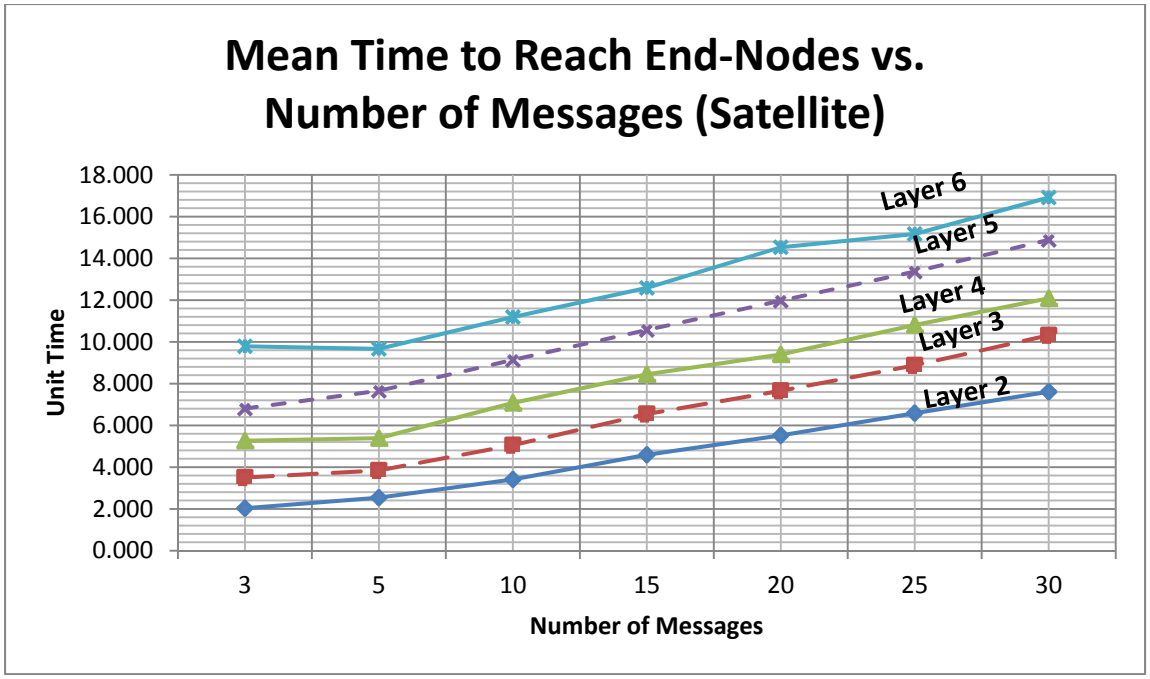

Figure 27. Trend Breakdown of Mean Time for Data-Packages to Reach End-Nodes for Varying Number of Layers of System Nodes (Satellite Model)

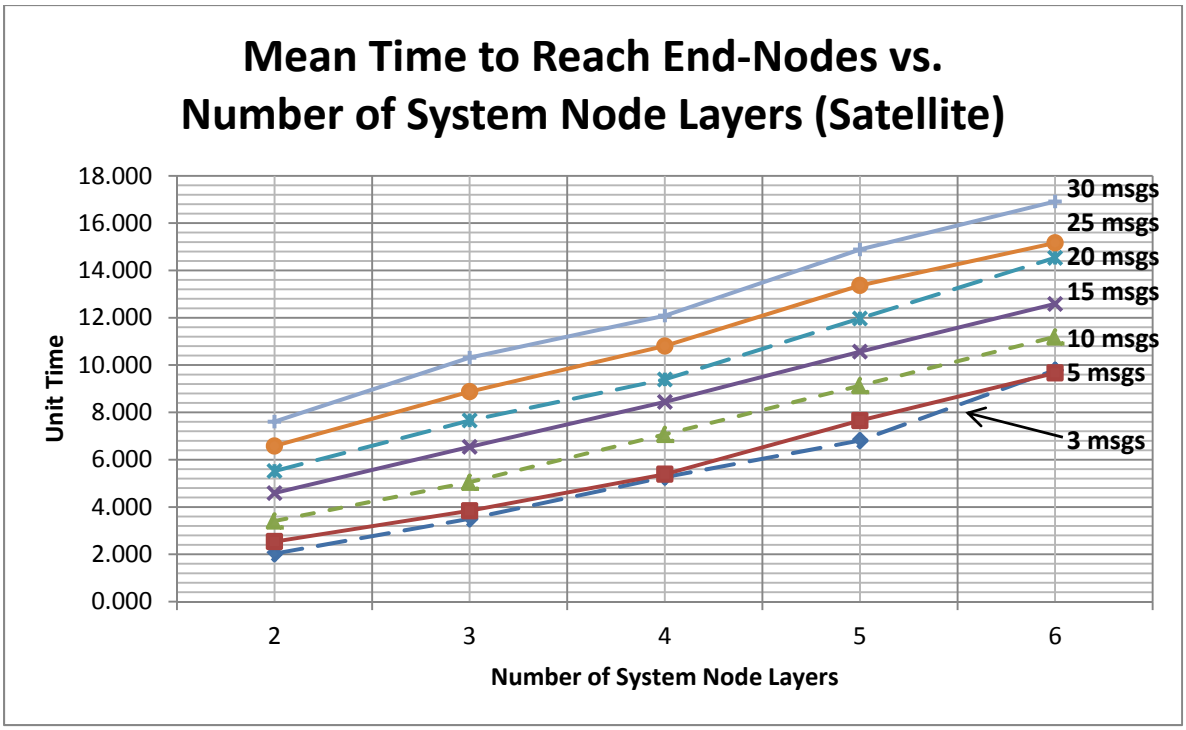

Figure 28. Trend Breakdown of Mean Time for Data-Packages to Arrive Back at Origin for Varying Number of Messages (Satellite Model)

#Msgs / #Layers	3	5	10	15	20	25	30	Remark(s)
2	4.615	5.939	10.420	14.813	19.115	23.804	23.779	3 nodes
3	7.968	11.306	21.840	30.560	39.615	47.932	57.113	7 nodes
4	14.791	23.980	46.260	64.460	84.095	97.760	117.717	15 nodes
5	30.751	49.925	97.170	134.627	178.510	212.588	248.670	31 nodes
6	62.158	101.524	200.530	294.760	377.660	451.340	527.297	63 nodes

Table 8. Average Elapsed Time to Propagate to End-Nodes and Return to Message Generating Node for Satellite Model

Although improvements were observed in the timeliness of end-nodes receiving propagated data/information packages, the direct sending of feedback packages to the Origin did not improve the time taken for the messages to arrive back at the message generating node, as observed in Table 6. and Table 8. . Thus, it would take the approximately the same time delay before the message generating node can send out a follow-up message to the system nodes for

further instructions. Nonetheless, this follow-up message will be able to arrive at the designated system node in the subsequent message dissemination in a shorter overall timeline. Thus, through changing the network transmission routes using additional communication channel(s), it is possible to shorten the overall message transmission time. To handle the increasing number of participating systems in the SoS and increasing number of targets in the environment, a secondary channel supporting the direct feedback of messages, such as a satellite link, would reduce the overall time delayed for messages to reach all systems and return to the originating system node.

Having no improvement to the time taken for messages to propagate the system nodes and returning to the originating node could be a limitation of the data processing capability of the Origin system node in handling the increased network traffic. The acknowledgement message returns to the Origin could be modified to make the simulation more realistic by reducing the processing time at system nodes, as they should occupy a smaller data size as compared to key data/information packages. The capability of the nodes in the system to receive, process and act on data/information sent from other system nodes should be a key consideration in systems integration design and planning, as this would impact inter-linking systems when individual system nodes could be sending data/information out at the same time.

Although potential delays may be incurred on the originating system node when receiving acknowledgement feedbacks from other nodes in the SoS network, these acknowledgement packages do not impact the operations of the other system nodes. In addition, in simulation runs on the new network architectural model, the introduction of the satellite communication channel allowed data/information to be delivered to the end-nodes in a largely improved timing. This greatly improved the overall SoS efficiency in reacting to rapidly evolving battlefield scenarios that require multi-system cooperation and a short response time.

E. DISCUSSION OF FUTURE WORK

The simulation models used to replicate SoS network architectures are inadequate in their simulation to real-life SoS networks. Improvements could be made on these models to gather more in-depth statistics of the SoS interoperability performance given a greater variety of modeling variables.

1. Possible Improvements to SoS Network Architecture Model

Several assumptions were made in the design and development of the SoS network architecture models designed and studied in Chapters VI and VII to generalize the performances and/or constraints of the individual system in terms of processing time with an ideal propagation delay of zero simulation time units. System nodes were also allocated a common set of characteristic processing times and processing capacity of three data/information packages every time. The data/information packages generated and propagated by the system nodes were also of the same size, requiring the same amount of time to process by the individual nodes. The medium of information propagation was also assumed to be fixed, thus no additional processing or delay time was incurred in the network model due to this.

These factors could be injected to the current network architectural models through correlating them with the modeling components available through ExtendSim. Some examples include:

- Delay factors within system nodes could be decomposed into smaller elements and listed in a tabular database to provide better resolution to the actual delays incurred at individual system nodes. Additional *Activity* blocks could also be built into the network model to model the time latency of information transmission between system nodes.
- Varying processing capabilities of individual system nodes could be modified through modifying their processing capabilities in the *Activity* blocks within each individual system.
- Data/information package sizes could be referenced to existing network message package type and size. Depending on the type of the package, data bytes could be allocated to the package based

on the data/information that the package would contain. The processing times of these messages could then be varied depending on their size and the processing capability of the system node.

- Data packet drops due to invalid data or time-outs (in which data/information package is no longer useful) could be incorporated into the ExtendSim models through modifications in the *Queue* and *Activity* blocks.

The precision of modeling systems is dependent on the precision of the input parameters and system characteristics. Without the necessary information available, it would be difficult to obtain accurate knowledge of the system through it's model. Thus, the more details that can be applied into the model, the more realistic and coherent the results will be with the real-world model.

2. Comparison with Other Network Architecture Models

Comparison studies could be conducted together with other types of network architecture models to evaluate the effectiveness of them handling the load of numerous systems and messages. Of interest is the network generating process described by Kawachi et al. (2004) as system nodes are re-linked to improve the performance of the system as a whole, with small average distances between nodes, with a bias such that links are moved to be adjacent to highly linked nodes (nodes of high degree). The network evolutions due to this method could be studied to evaluate the possible security risks involved and the system downtime or loss of information during re-linkages between subsystems.

Dekker (2005) had described a new agent-based simulation system to study the impact of network topology (with networks developed from the process proposed by Kawachi et al.) on military combat effectiveness. The parameters, such as average distance, clustering coefficient and node connectivity, used to characterize the network models could be applied to the network models studied in this thesis and together with other potential network models so that the network architecture with the better performance could be chosen over others.

3. Quality Loss Function Analysis

A general quality loss function which can be utilized to justify a decision on how much to invest to improve a process that is already capable of meeting requirements was developed by Don Oh and Langford (2008). This loss function could also be applied to evaluate the performance of the system (in terms of amount of time delay incurred between systems) versus the number of systems in the SoS network. This could provide insight into how much delay should be expected in a network of systems if there were to be that many numbers of systems participating in the data communications. The same could be done between performance of the system and the number of messages sent over these systems.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSION

Systems in the world today are becoming more interconnected and complex, so as to achieve much more together than if they were on their own. However, to achieve the ideal end-state of smooth interoperability, it is important to understand what are the issues needed to be managed before solutioning can occur. An analogy was drawn between interoperability of systems and the inter-relationships between humans at work, which helped identify the factors that could affect the effectiveness and efficiency of system-to-system interoperability. These elements include command and control ontology to provide a framework to facilitate and regulate information exchange, local and global system stability, command and control of the systems and trust to enable C2.

These factors were examined with regards to the problem of establishing and maintaining interoperability in a target-rich environment. Process decomposition was used to identify key processes to address interoperability, namely network architecture, C2, common ontology, systems integration, systems stability, information security, concept of operations and management of change requirements.

To further study the issue of increasing number of systems in the SoS network and an increasingly congested environment, a network model was designed and developed in ExtendSim to simulate the transmission of data/information package(s) in a SoS network of multiple nodes and assess the factors causing the time delay in sending messages. The time delay or time taken for messages to reach intended system node(s) would influence the both the accuracy of the data/information sent and time remaining for the subsystem to react on the target.

In the first version of the network model, a single channel, in which the data transmission and feedback was sent via the same channel, was used to propagate data/information messages from the message generating system

node to the rest of the nodes in the constructed network and back to the originating node. This simulated the connection, coupling and cohesion of the communications between the message sending system to the other systems as feedback messages are sent in reply to the sent messages from the message generating system. It was found that the number of layers of system nodes had a more profound impact on the timeliness of the messages arriving at the end-nodes than compared with the number of messages being propagated through the SoS network. The message traverse time increased exponentially with an increased number of system node layers. A similar observation was made on the time taken for data/information packages to traverse from the message generating node to the end-nodes and back to the originating node.

The single-channel data transmission model was modified into a dual-channel data transmission network model through the addition of a separate path for feedback transmission back to the originating system node. With this change, the time taken to send the messages to the end system nodes from the message generating node was greatly reduced. The traverse time profile becomes linearized as compared to an exponential increase, as the network traffic of the messages sent from the message generating node to the end-nodes is not affected by the feedback return as the feedback has been re-routed to a direct link (e.g., via satellite communications) back to the originating system node. This illustrates an improvement in the time delay for data/information to reach the end system nodes. However, this direct routing of the feedback loop to the originating system node did not improve the time taken for the messages to arrive back at the message generating node, indicating that it would take approximately the same time delay before the message generating node can send out a follow-up message to the system nodes for further instructions. Nonetheless, this follow-up message will be able to arrive at the designated system node in the subsequent message dissemination in a shorter overall timeline. Thus, through changing the network transmission routes using additional communication channel(s), it is possible to shorten the overall message transmission time. To handle the

increasing number of participating systems in the SoS and increasing number of targets in the environment, a secondary channel supporting the direct feedback of messages, such as a satellite link, would reduce the overall time delayed for messages to reach all systems and return to the originating system node.

Future works include parameter modifications to the existing network models to make them more realistic and applicable to other types of information transmission, comparison of the network models against other types of network models and performing quality loss function analysis on existing results to examine how much stakeholders are willing to pay for modifications to C2 network architectures to improve its performance, and thus support critical decision making.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I: SUGGESTED ELEMENTS OF AN ADVANCED NAVAL INFORMATION ASSURANCE RESEARCH PROGRAM

Program Element	Description
Network Level	• *Border Gateway Protocol/Domain Name Service protocol "hardening"*—core network protocols responsible for routing and naming services for all Internet Protocol traffic. • *Network filtering*—filtering strategies to detect incoming attacks as well as outgoing exfiltration of sensitive information. • *Network visualization*—tools for alerting network operation to attack conditions. • *Resilient networks*—networks to ensure continual service while under denial-of-service attacks. • *Source attribution*—tools for ascertaining where a connection or attack is actually coming from. • *Decoy networking*—strategy to lure an adversary to an isolated network from which it can be monitored for intelligence (methods, behavior, and sources).
System Level	• *Secure composition*—means to ensure security properties of the whole system. • *Artificial diversity*—techniques to diversify computing fabric that allows interoperability, but also allows a change in structure of the same software for another implementation. • *Collaborative software communities*—a sharing of attack data to harden other instances of software against in-progress attacks and developing related security alert sharing technologies. • *Privacy-preserving technologies*—technologies to allow effective sharing of data while maintaining strict compartmentalization.
Host Level	• *Counter-evasion techniques for obfuscated malware*—methods to identify malware-embedded content flows. • *Virtualization for security*—technology for server consolidation and isolation of untrusted applications from the host operating system. • *Self-healing software*—software that monitors and models its own behavior. • *Hardware life-cycle tamper resistance*—techniques to detect compromises in chip-level designs and implementations during supply chain life-cycle attacks.

User Level	• *Behavior-based security*—analysis of user behavior patterns to detect threats with reasonably high reliability. • *Defense through uncertainty*—leveraging uncertainty in deployed environments to make exploitation difficult by adversary.
Privileged-User Level	• *Role and behavior-based access control*—means of associating logical roles of a user with the specific data and applications used by the specific roles defined with an enterprise and a means of granting access to network resources. • *Self-protecting security technologies*—means of preventing denial-of-service attacks caused by a user accidentally or by design.

Table 9. Information Assurance Elements (From Committee on Information Assurance for Network-Centric Naval Forces, 2010, p. 89)

APPENDIX II

A. EXTENDSIM MODELS FOR VARYING LAYERS OF SYSTEM NODES IN SINGLE-CHANNEL FOR DATA EXCHANGE

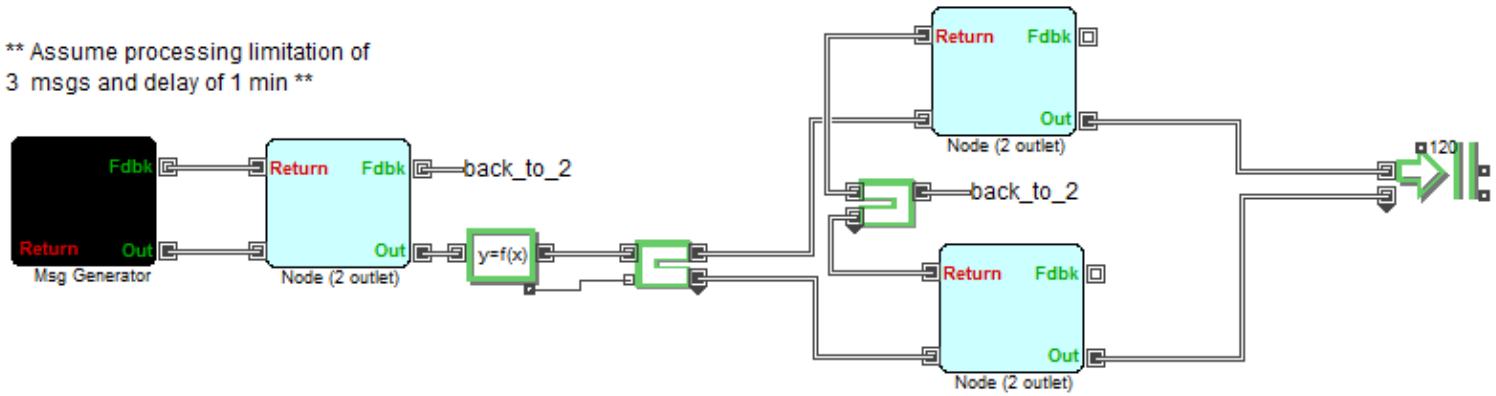

Figure 29. ExtendSim Network Model of 3 Generic System Nodes (2 Layers)

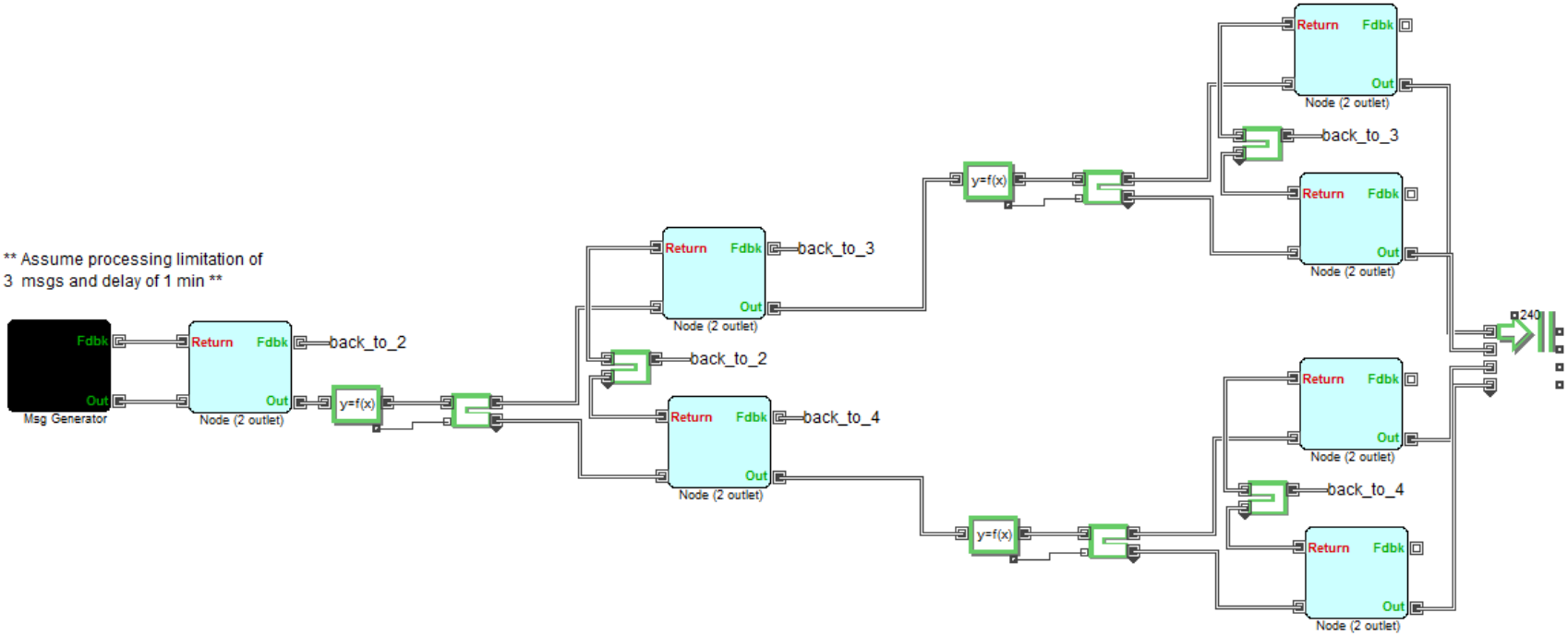

Figure 30. ExtendSim Network Model of 7 Generic System Nodes (3 Layers)

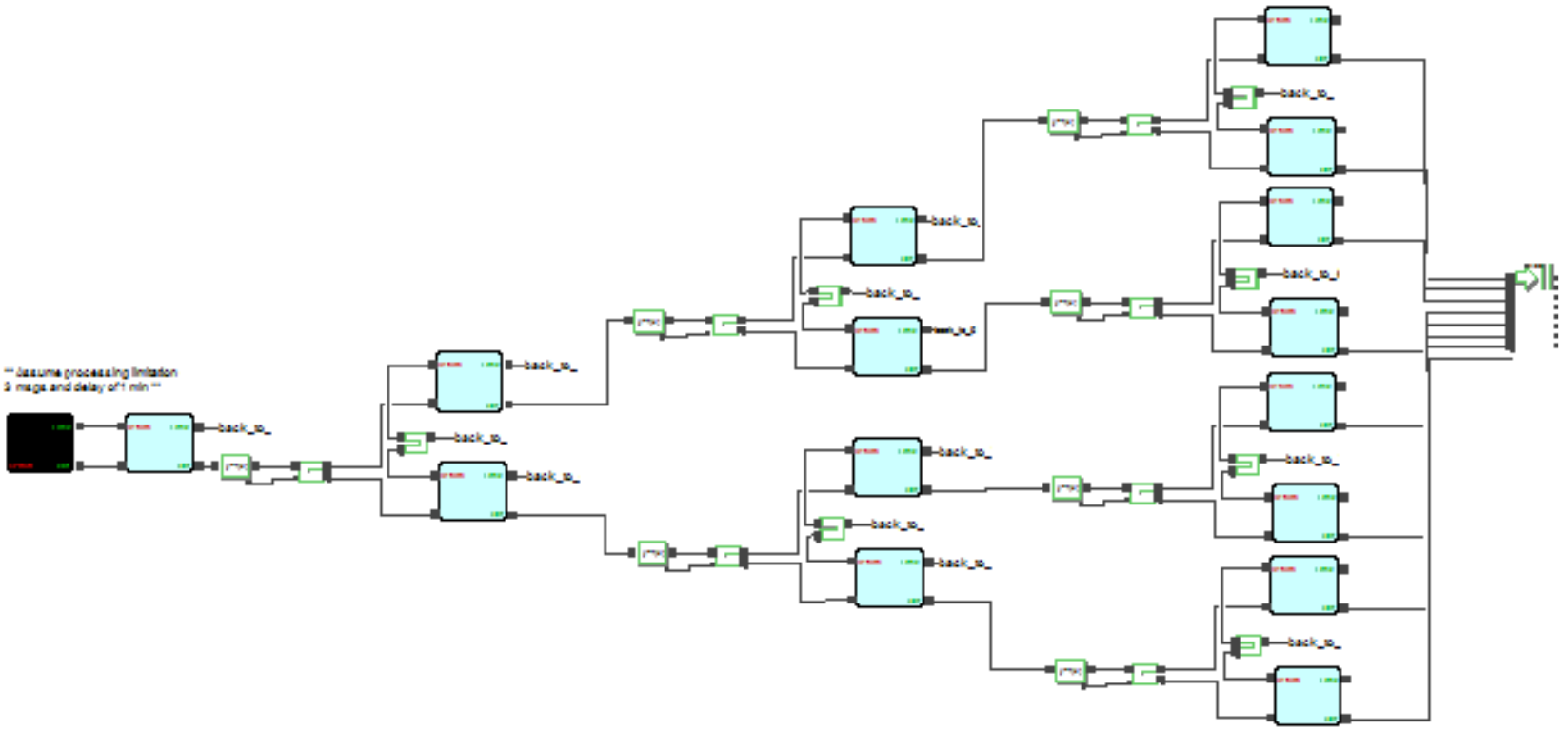

Figure 31. ExtendSim Network Model of 15 Generic System Nodes (4 Layers)

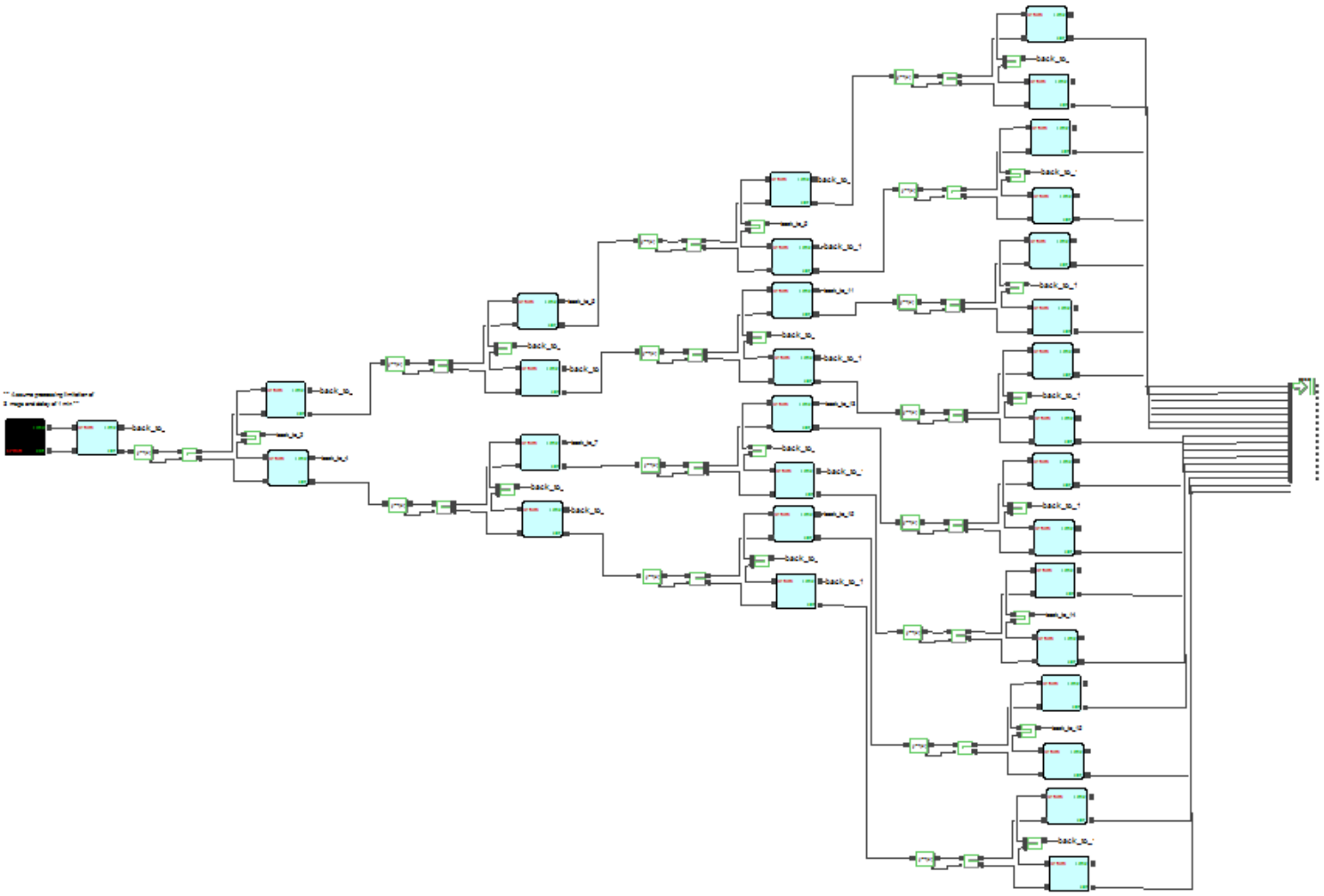

Figure 32. ExtendSim Network Model of 31 Generic System Nodes (5 Layers)

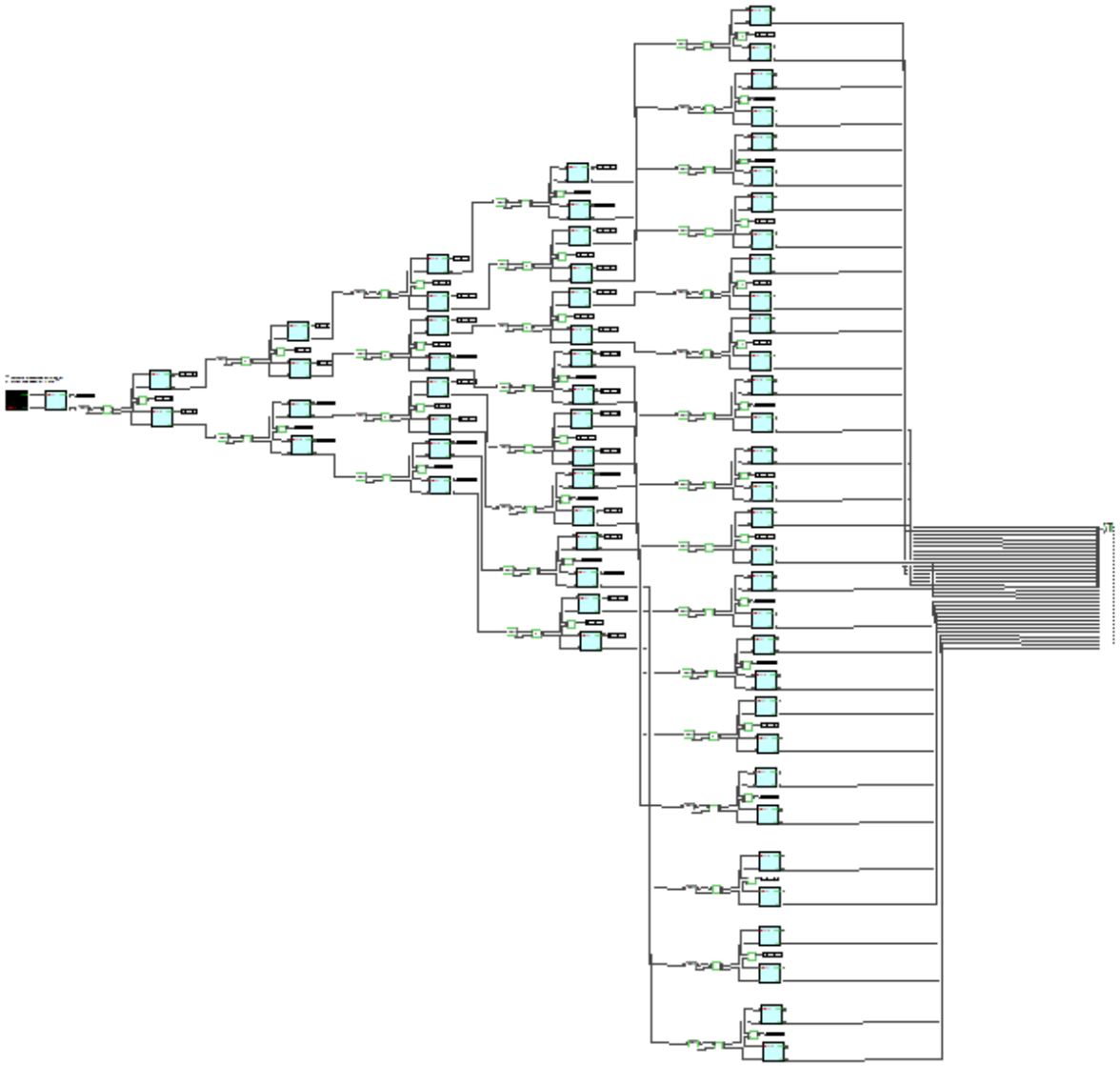

Figure 33. ExtendSim Network Model of 63 Generic System Nodes (6 Layers)

B. EXTENDSIM MODELS FOR VARYING LAYERS OF SYSTEM NODES IN DUAL-CHANNELS FOR DATA EXCHANGE

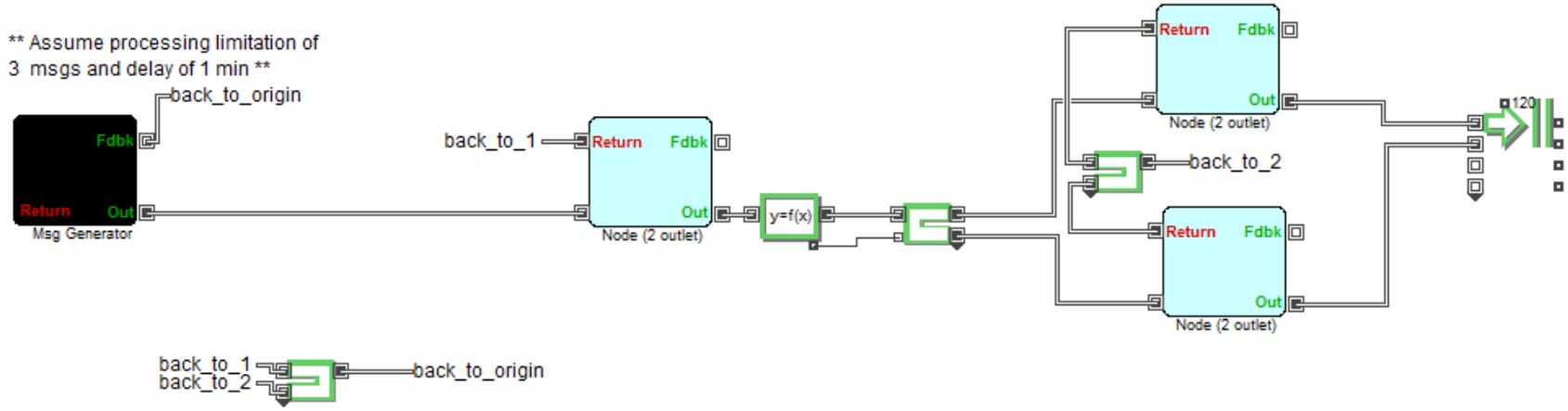

Figure 34. Modified ExtendSim Network Model of 3 Generic System Nodes (2 Layers)

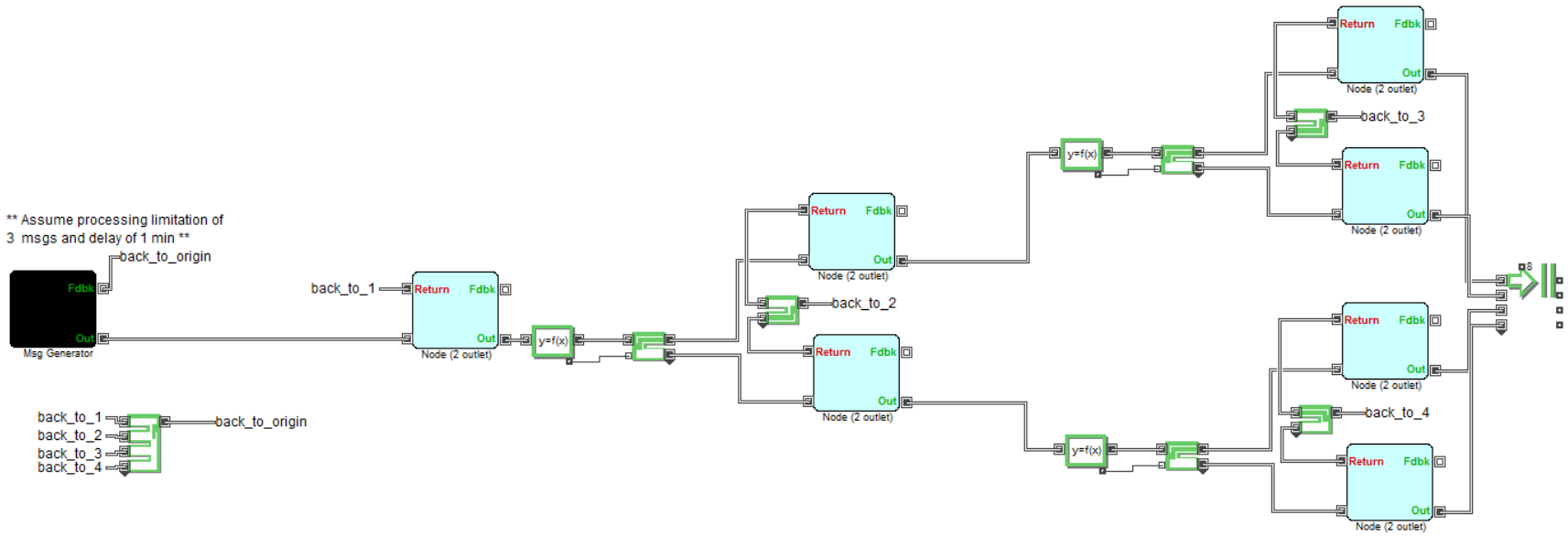

Figure 35. Modified ExtendSim Network Model of 7 Generic System Nodes (3 Layers)

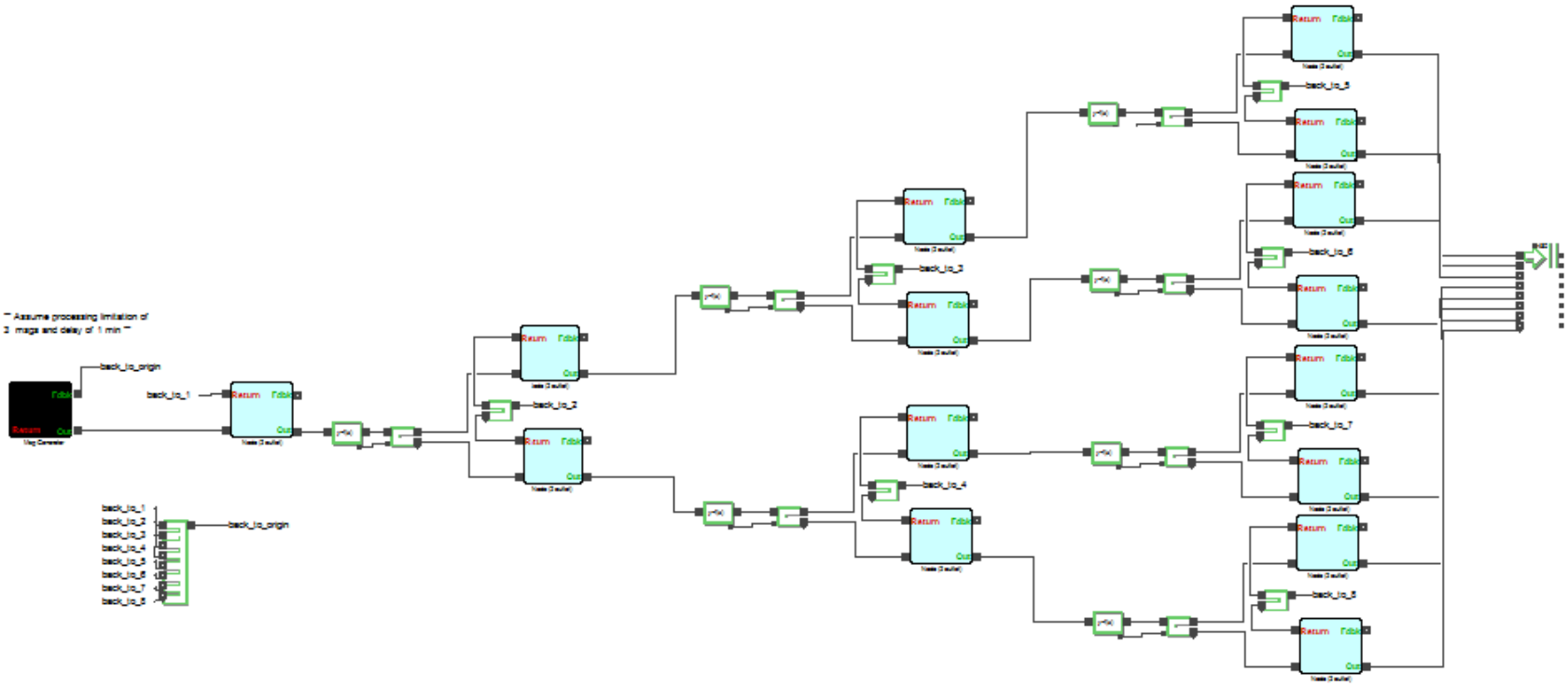

Figure 36. Modified ExtendSim Network Model of 15 Generic System Nodes (4 Layers)

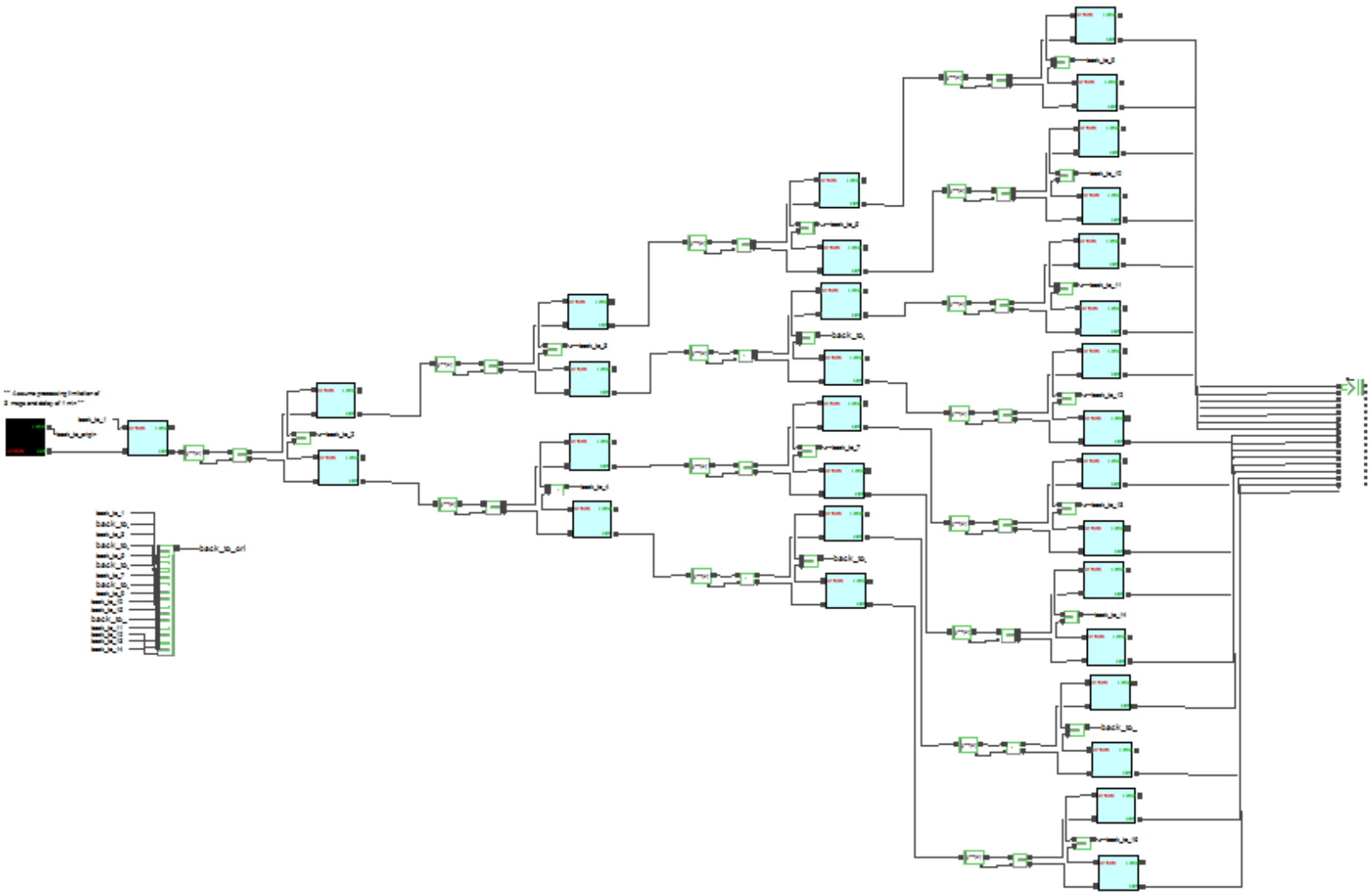

Figure 37. Modified ExtendSim Network Model of 31 Generic System Nodes (5 Layers)

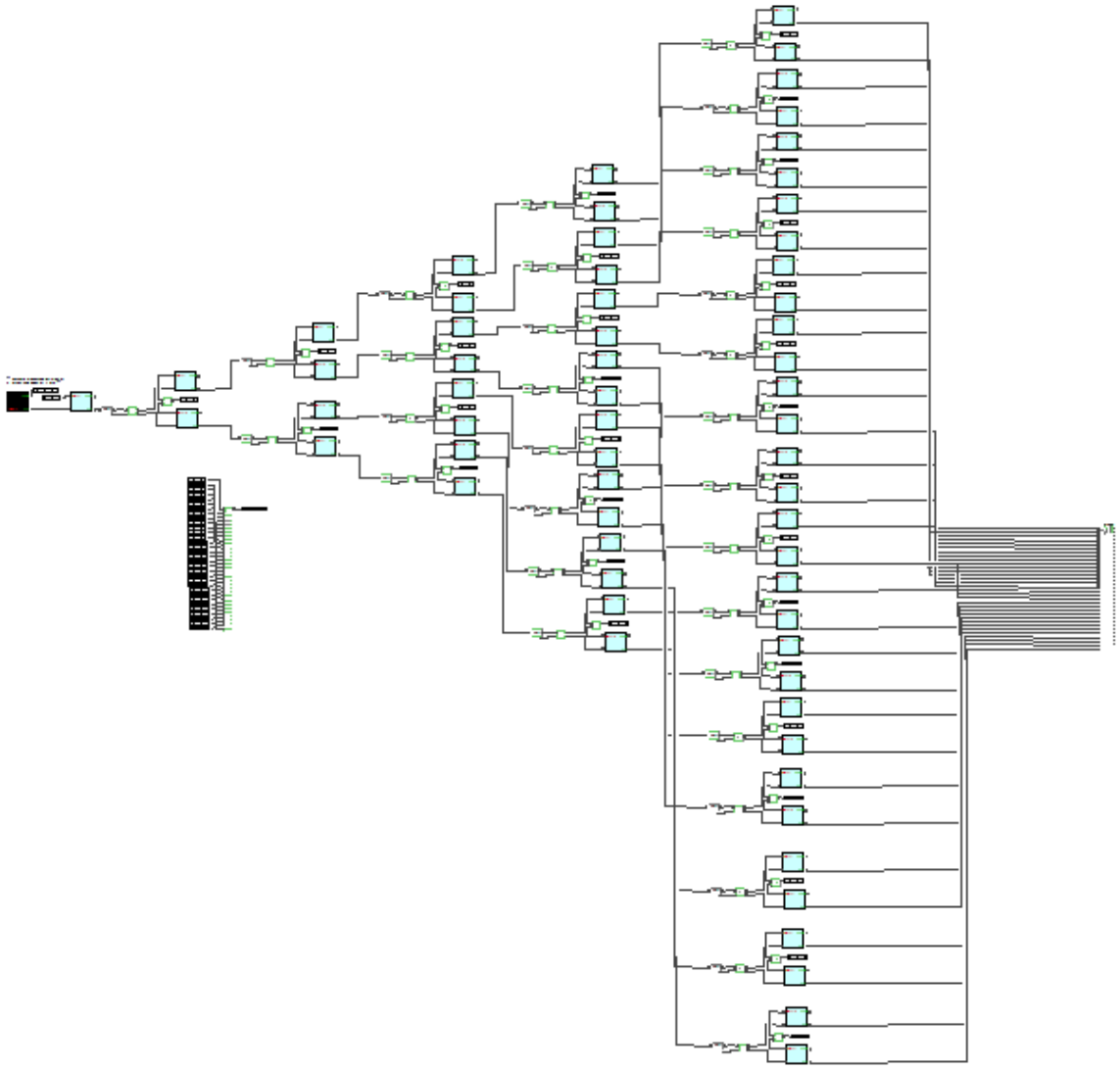

Figure 38. Modified ExtendSim Network Model of 63 Generic System Nodes (6 Layers)

LIST OF REFERENCES

Alberts, D. S., & Hayes, R. E. (2003). *Power to the Edge: Command and Control in the Information Age.* Washington, DC: DoD Command and Control Research Program.

Alberts, D. S., & Hayes, R. E. (2006). *Understanding Command and Control.* Washington, DC: DoD Command and Control Research Program.

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network Centric Warfare: developing and leveraging information superiority.* Washington, DC: DoD C4ISR Cooperative Research Program.

Chapter 5: Topology. (2012, August 26). From Florida Center for Instructional Technology: http://fcit.usf.edu/network/chap5/chap5.htm

Chief of Naval Operations Staff (OPNAV), Office of the. (2008, October). *Naval Open Architecture Strategy.* Retrieved from Acquisition Community Connection: https://acc.dau.mil/CommunityBrowser.aspx?id=129676&lang=en-U.S.

Committee on Information Assurance for Network-Centric Naval Forces. (2010). *Information Assurance for Network-Centric Naval Forces.* Washington, DC: The National Academies Press.

Communication. (n.d.). Retrieved from Dictionary.com: http://dictionary.reference.com/browse/communication

Defense Acquisition University. (n.d.). *Concept of Operations (CONOPS)*. Retrieved from ACQuipedia: https://acc.dau.mil/CommunityBrowser.aspx?id=28869&view=w

Dekker, A. H. (December 2005). Network Topology and Military Performance. *MODSIM 2005 International Congress on Modelling and Simulation*, 2174–2180.

Department of Defense. (2003). *Joint Operations Concepts.* Washington, DC: Author.

Department of Defense. (2007). *DoD Architecture Framework Version 1.5.* Washington, DC: Author.

Department of Defense. (2009). *FY2009–2034 Unmanned Systems Integrated Roadmap.* Washington, DC: Author.

Department of Defense. (2011). *Unmmaned Systems Integrated Roadmap FY2011–2036.* Washington, DC: Author.

Department of Defense, Office of Force Transformation. (2005). *The Implementation of Network-Centric Warfare.* Washington, DC: Government Printing Office.

Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering, Office of the. (2008). *Systems Engineering Guide for Systems of Systems, Version 1.0*. Washington, DC: ODUSD(A&T)SSE.

Ding, X. C. (2009). *Real-Time Optimal Control of Autonomous Switched Systems.* (PhD Thesis, Georgia Institute of Technology).

Don Oh, C., & Langford, G. (2008). *A General Quality Loss Function Development and Application to the Acquisition Phases of the Weapon Systems.* (Masters Thesis, Naval Postgraduate School).

Gideon, J. M., Dagli, C. H., & Miller, A. (2005). Taxonomy of Systems-of-Systems. *Proceedings of the Conference on Systems Engineering Research 2005*, 356–363. Hoboken, NJ: Stevens Institute of Technology.

Gruber, T. (n.d.). *What is an Ontology?* Retrieved from Knowledge Systems, AI Laboratory, Stanford University: http://www-ksl.stanford.edu/kst/what-is-an-ontology.html

Heterogeneous. (n.d.). Retrieved from Dictionary.com: http://dictionary.reference.com/browse/heterogeneous

Hitachi Cable Manchester. (2012, August 27). *What is Open Architecture?* From Accu-Tech: http://www.accu-tech.com/Portals/54495/docs/Open%20Vs%20Closed%20Architecture.pdf

Hsieh, C. Y. (n.d.). *Lesson 3: Network Topology*. Retrieved from Knowledge Systems Institute, Graduate School of Computer & Information Sciences: http://pluto.ksi.edu/~cyh/cis370/ebook/ch01d.htm

Hsieh, C. Y. (2012, August 27). *Lesson 3: Network Topology*. From Knowledge Systems Institute, Graduate School of Computer & Information Sciences: http://pluto.ksi.edu/~cyh/cis370/ebook/ch01d.htm

Imagine That Inc. (2010). ExtendSim 8 User Manual*.* San Jose, CA: Imagine That Inc.

Jin, Z. (2007). *Coordinated Control for Networked Multi-Agent Systems.* (PhD Thesis, California Institute of Technology).

Johnson, C. W. (n.d.). *What are Emergent Properties and How Do They Affect the Engineering of Complex Systems?* Retrieved from Department of Computing Science, University of Glasgow: http://www.dcs.gla.ac.uk/~johnson/papers/emergence.pdf

Joint Chiefs of Staff. (2001, September 10). *Joint Publication 3–0, Doctrine for Joint Operations.* Retrieved from U.S. Forest Service: http://www.fs.fed.us/fire/doctrine/genesis_and_evolution/source_materials/dod_joint_ops_doctrine.pdf

Joint Chiefs of Staff. (2010, November 8). *Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms.* Retrieved from Defense Technical Information Center: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Joint Chiefs of Staff. (2012, March 21). *Chairman of the Joint Chiefs of Staff Instruction (CJCSI).* Retrieved from Defense Technical Information Center: http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf

Kawachi, Y., Murata, K., Yoshii, S., & Kakazu, Y. (2004). The structural phase transition among fixed cardinal networks. *Proceedings of the 7th Asia-Pacific Conference on Complex Systems*, 247–255. Cairns, Australia.

Langford, G. O. (2012). Engineering Systems Integration - Theory, Metrics, and Methods. CRC Press.

Liebowitz, S. J., & Margolis, S. E. (n.d.). *Network Externalities (Effects).* Retrieved from The University of Texas at Dallas: http://www.utdallas.edu/~liebowit/palgrave/network.html

Maier, M. W. (n.d.). *Architecting Principles for Systems-of-Systems.* Retrieved from Info|Ed: http://www.infoed.com/Open/PAPERS/systems.htm

Maier, M. W., & Rechtin, E. (2009). The Art of Systems Architecting (3rd ed.). CRC Press.

Nelson, E. M. (2008, September 30). *Open Architecture Technical Principles and Guidelines*. (1.5.8).

North Atlantic Treaty Organization. (2012, May 10). *NATO Integrated Air and Missile Defence*. Retrieved from North Atlantic Treaty Organization: http://www.nato.int/cps/en/natolive/topics_8206.htm

Pawar, D. (2008, March 6). *Types of Network Topology*. Retrieved from Ezine @rticles: http://ezinearticles.com/?Types-of-Network-Topology&id=1029087

Pigeau, R., & McCann, C. (2002). Re-Conceptualizing Command and Control. *Canadian Military Journal*, 53–64.

Policies and Procedures. (n.d.). Retrieved from BusinessDictionary.com: http://www.businessdictionary.com/definition/policies-and-procedures.html

Quincy, K. E., Thompson, B. G., Moran, M. G., Nilsson, D. J., & Johnson, J. J. (2010). *An Integrated Command and Control Architecture Concept for Unmanned Systems in the Year 2030.* (Masters Thesis, Naval Postgraduate School).

Rechtin, E. (1991). Systems Architecting: Creating & Building Complex Systems. Los Angeles, CA: Prentice Hall.

Research and Technology Organisation, North Atlantic Treaty Organisation. (2004). *NATO Code of Best Practice for Command and Control Assessment.* Châtillon Cedex, France.

Rouse, M. (2005, April). *Definition - CPI*. Retrieved from WhatIs.com: http://whatis.techtarget.com/definition/CPI

Rumsfeld, D. H., (2003). Secretary's Foreward. *Transformation Planning Guide*. Washington, DC: Author.

Skyttner, L. (2005). Systems theory and the science of military command and control. *Kybernetes, 34* (7), 1240–1260.

Sturdy, J. T. (June 2004). *Military Data Link Integration Application.* Albuquerque, NM: Honeywell Defense and Space Electronic Systems.

Under Secretary of Defense for Acquisition, Technology, and Logistics, Office of the. (2009). *Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise.* Washington, DC: Author.

Weisstein, E. W. (2012, August 23). *Exponential Distribution*. From Wolfram MathWorld: http://mathworld.wolfram.com/ExponentialDistribution.html

GENERAL READING REFERENCES

Alberts, D. S., & Hayes,. E. (2007). Planning: Complex Endeavors. Washington, DC: DoD Command and Cotrol Research Program.

Beardmore, R. (2006, February 17). *Control System Stability*. Retrieved from RoyMech: http://www.roymech.co.uk/Related/Control/Stability.html

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Gary O. Langford
   Naval Postgraduate School
   Monterey, California

4. Professor Oleg A. Yakimenko
   Naval Postgraduate School
   Monterey, California

5. Dr. John S. Osmundson
   Naval Postgraduate School
   Monterey, California

6. Professor Joseph Rice
   Naval Postgraduate School
   Monterey, California

7. Teo Tiat Leng (Mr)
   Deputy Director LS
   Defence Science and Technology Agency, Singapore
   Singapore, Singapore

8. Professor Yeo Tat Soon
   Director
   Temasek Defence Systems Institute
   National University of Singapore
   Singapore

9. Tan Lai Poh (Ms)
   Senior Manager
   Temasek Defence Systems Institute
   National University of Singapore
   Singapore

10. Pang Chung Kiang (Mr)
Director DMSA
Defence Science and Technology Agency, Singapore
Singapore